

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN**

AUTHENTICOM, INC.,

Plaintiff,

Case No. 17-cv-318-jdp

v.

CDK GLOBAL, LLC, and THE REYNOLDS
AND REYNOLDS COMPANY,

Defendants.

**AUTHENTICOM'S CONSOLIDATED OPPOSITION TO
DEFENDANTS' RULE 12(b)(6) MOTIONS TO DISMISS**

TABLE OF CONTENTS

	Page
INTRODUCTION	1
FACTUAL BACKGROUND	4
I. Parties and Industry Background	4
II. The Horizontal Conspiracy Between CDK and Reynolds	9
III. Restrictive Vertical Agreements	14
IV. Harm to Competition	15
V. Authenticom Does Not Compromise Defendants' Data Security or System Integrity	17
VI. Harm to Authenticom	18
ARGUMENT	19
I. Authenticom Has Stated Plausible Claims Under Section 1 of the Sherman Act	19
A. The Complaint Alleges a Per Se Unlawful Horizontal Conspiracy	19
1. Defendants Agreed To Block Independent Integrators and Drive Them from the Market	19
2. The February 2015 Agreements Unlawfully Divide the Data Integration Market Between CDK and Reynolds	23
B. The Complaint Alleges Unlawful Exclusive Dealing	26
1. Defendants' Exclusive Dealing Terms Foreclose Authenticom from a Substantial Portion of the Data Integration Market	27
2. The Effect of Defendants' Exclusive Dealing Terms Has Been Supra-Competitive Pricing and Reduced Output	29
C. The Complaint Alleges Unlawful Tying	35
II. Authenticom Has Stated a Plausible Monopolization Claim Under Section 2 of the Sherman Act	39
A. The Complaint Pleads That Defendants Have Market Power in Their Respective Data Integration Aftermarkets	39
B. The Complaint Adequately Pleads That Defendants Acquired and Maintain Their Market Power Through Anticompetitive Means	46
III. The Computer Fraud and Abuse Act Does Not Defeat Authenticom's Claims	47
IV. Authenticom Has Stated a Plausible Claim for Tortious Interference	54
CONCLUSION	55

TABLE OF AUTHORITIES

CASES	Page
<i>42nd Parallel N. v. E St. Denim Co.</i> , 286 F.3d 401 (7th Cir. 2002)	37
<i>ABS Global, Inc. v. Inguran, LLC</i> , 2016 WL 3963246 (W.D. Wis. 2016).....	28
<i>Allied Orthopedic Appliances Inc. v. Tyco Health Care Grp. LP</i> , 592 F.3d 991 (9th Cir. 2010)	33, 34
<i>American Needle, Inc. v. NFL</i> , 560 U.S. 183 (2010).....	26, 38
<i>Andrx Pharm., Inc. v. Biovail Corp. Int'l</i> , 256 F.3d 799 (D.C. Cir. 2001)	26
<i>Assessment Techs. of Wis., LLC v. WIREdata, Inc.</i> , 350 F.3d 640 (7th Cir. 2003)	50
<i>AtPac, Inc. v. Aptitude Sols., Inc.</i> , 730 F. Supp. 2d 1174 (E.D. Cal. 2010).....	52
<i>Avaya Inc. v. Telecom Labs, Inc.</i> , 2014 WL 2940455 (D. N.J. June 30, 2014)	44
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	1
<i>Blizzard Entm't Inc. v. Ceiling Fan Software LLC</i> , 941 F. Supp. 2d 1227 (C.D. Cal. 2013)	45
<i>Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic</i> , 152 F.3d 588 (7th Cir. 1998)	24
<i>Briggs & Stratton Corp. v. Kohler Co.</i> , 405 F. Supp. 2d 986 (W.D. Wis. 2005)	39
<i>Bubis v. Blanton</i> , 885 F.2d 317 (6th Cir. 1989)	51
<i>Burbank Grease Servs., LLC v. Sokolowski</i> , 717 N.W.2d 781 (Wis. 2006).....	54

<i>Burda v. Wendy's Int'l, Inc.,</i> 659 F. Supp. 2d 928 (S.D. Ohio 2009)	44
<i>C.R. Bard, Inc. v. M3 Sys., Inc.,</i> 157 F.3d 1340 (Fed. Cir. 1998).....	34
<i>Canadian Import Antitrust Litig., In re,</i> 470 F.3d 785 (8th Cir. 2006)	51
<i>Carl Sandburg Vill. Condo. Ass'n No. 1 v. First Condo. Dev. Co.,</i> 758 F.2d 203 (7th Cir. 1985)	36
<i>Child Evangelism Fellowship of Minn. v. Elk River Area Sch. Dist. #728,</i> 599 F. Supp. 2d 1136 (D. Minn. 2009).....	21
<i>Collins Inkjet Corp. v. Eastman Kodak Co.,</i> 2014 WL 11516553 (S.D. Ohio 2014), <i>aff'd</i> , 781 F.3d 264 (6th Cir. 2015).....	41
<i>Consolidated Exp., Inc. v. New York Shipping Ass'n, Inc.,</i> 602 F.2d 494 (3d Cir. 1979), <i>rev'd on other grounds</i> , 448 U.S. 902 (1980).....	48
<i>Conwood Co. v. U.S. Tobacco Co.,</i> 290 F.3d 768 (6th Cir. 2002)	47
<i>Dairy Farmers of Am., Inc. Cheese Antitrust Litig., In re,</i> 767 F. Supp. 2d 880 (N.D. Ill. 2011)	45-46
<i>Datel Holdings Ltd. v. Microsoft Corp.,</i> 712 F. Supp. 2d 974 (N.D. Cal. 2010)	44
<i>Dos Santos v. Columbus-Cuneo-Cabrini Med. Ctr.,</i> 684 F.2d 1346 (7th Cir. 1982)	38
<i>EF Cultural Travel BV v. Zefer Corp.,</i> 318 F.3d 58 (1st Cir. 2003).....	49
<i>Eastman Kodak Co. v. Image Tech. Servs.,</i> 504 U.S. 451 (1992).....	3, 35, 36, 39, 40, 41, 42, 44, 45, 46
<i>Eli Lilly & Co. v. Arla Foods Inc.,</i> 2017 WL 2976697 (E.D. Wis. July 11, 2017)	21

Facebook, Inc. v. Power Ventures, Inc.:

2013 WL 5372341 (N.D. Cal. Sept. 25, 2013),	53
844 F.3d 1058 (9th Cir. 2016), <i>pet. for cert. pending</i> , No. 16-1105 (U.S. filed Mar. 9, 2017).....	53
<i>Finch v. Southside Lincoln-Mercury, Inc.</i> , 685 N.W.2d 154 (Wis. Ct. App. 2004)	54
<i>Geinosky v. City of Chicago</i> , 675 F.3d 743 (7th Cir. 2012)	4, 19
<i>Gen. Leaseways, Inc. v. Nat'l Truck Leasing Ass'n</i> , 744 F.2d 588 (7th Cir. 1984)	24-25
<i>Girl Scouts of Manitou Council, Inc. v. Girl Scouts of U.S. of Am., Inc.</i> , 549 F.3d 1079 (7th Cir. 2008)	21
<i>Gumwood HP Shopping Partners, L.P. v. Simon Prop. Grp., Inc.</i> , No. 3:11-CV-268	46
<i>Hardy v. City Optical Inc.</i> , 39 F.3d 765 (7th Cir. 1994)	37
<i>hiQ Labs, Inc. v. LinkedIn Corp.</i> , 2017 WL 3473663 (N.D. Cal. 2017)	49, 50
<i>High Fructose Corn Syrup Antitrust Litig., In re</i> , 295 F.3d 651 (7th Cir. 2002)	20
<i>Illinois Tool Works Inc. v. Indep. Ink, Inc.</i> , 547 U.S. 28 (2006).....	28
<i>Int'l Union, UAW v. NLRB</i> , 459 F.2d 1329 (D.C. Cir. 1972).....	30
<i>Jefferson Par. Hosp. Dist. No. 2 v. Hyde</i> , 466 U.S. 2 (1984).....	28, 35, 36
<i>Jurista v. Amerinox Processing, Inc.</i> , 492 B.R. 707 (D. N.J. 2013)	21
<i>K.M.B. Warehouse Distrib., Inc. v. Walker Mfg. Co.</i> , 61 F.3d 123 (2d Cir. 1995).....	37

<i>King Drug Co. of Florence, Inc. v. Smithkline Beecham Corp.</i> , 791 F.3d 388 (3d Cir. 2015), cert. denied, 137 S. Ct. 446 (2016).....	29
<i>Klor's, Inc. v. Broadway-Hale Stores, Inc.</i> , 359 U.S. 207 (1959).....	20, 23
<i>Lamp Liquors, Inc. v. Adolph Coors Co.</i> , 563 F.2d 425 (10th Cir. 1977)	48
<i>Lerma v. Univision Commc'ns, Inc.</i> , 52 F. Supp. 2d 1011 (E.D. Wis. 1999).....	46
<i>Liebe v. City Fin. Co.</i> , 295 N.W.2d 16 (Wis. Ct. App. 1980)	55
<i>Maltz v. Sax</i> , 134 F.2d 2 (7th Cir. 1943)	48, 51
<i>Matsushita Elec. Indus. Co. v. Zenith Radio Corp.</i> , 475 U.S. 574 (1986).....	22
<i>McWane, Inc. v. FTC</i> , 783 F.3d 814 (11th Cir. 2015), cert. denied, 136 S. Ct. 1452 (2016).....	31
<i>Memorex Corp. v. IBM Corp.</i> , 555 F.2d 1379 (9th Cir. 1977)	48
<i>Methodist Health Servs. Corp. v. OSF Healthcare Sys.</i> , 2016 WL 5817176 (C.D. Ill. 2016), aff'd, 859 F.3d 408 (7th Cir. 2017).....	27, 46
<i>Metso Minerals Indus., Inc. v. FLSmidth-Excel LLC</i> , 2010 WL 55845 (E.D. Wis. Jan. 5, 2010).....	55
<i>Motorola, Inc. v. Pick</i> , 2004 WL 5472092 (C.D. Cal. June 22, 2004)	21
<i>Nat'l Soc'y of Prof'l Eng'rs v. United States</i> , 435 U.S. 679 (1978).....	20
<i>New York ex rel. Schneiderman v. Actavis PLC</i> , 787 F.3d 638 (2nd Cir. 2015).....	34
<i>N. Pac. Ry. Co. v. United States</i> , 356 U.S. 1 (1958).....	35

<i>Nw. Wholesale Stationers, Inc. v. Pac. Stationery & Printing Co.,</i> 472 U.S. 284 (1985).....	20
<i>Novell, Inc. v. Microsoft Corp.,</i> 731 F.3d 1064 (10th Cir. 2013)	47
<i>Omnicare, Inc. v. UnitedHealth Grp., Inc.,</i> 629 F.3d 697 (7th Cir. 2011)	22
<i>Palmer v. BRG of Georgia, Inc.,</i> 498 U.S. 46 (1990).....	24, 26
<i>Perma Life Mufflers, Inc. v. Int'l Parts Corp.,</i> 392 U.S. 134 (1968).....	48
<i>Phillips v. Prudential Ins. Co. of Am.,</i> 714 F.3d 1017 (7th Cir. 2013)	19
<i>Pinto Trucking Serv., Inc. v. Motor Dispatch, Inc.,</i> 649 F.2d 530 (7th Cir. 1981)	48
<i>Ploss v. Kraft Foods Grp., Inc.,</i> 197 F. Supp. 3d 1037, 1070 (N.D. Ill. 2016)	29
<i>Premier Elec. Constr. Co. v. Nat'l Elec. Contractors Ass'n, Inc.,</i> 814 F.2d 358 (7th Cir. 1987)	26
<i>PSI Repair Servs., Inc. v. Honeywell, Inc.,</i> 104 F.3d 811 (6th Cir. 1997)	43
<i>Queen City Pizza, Inc. v. Domino's Pizza, Inc.,</i> 124 F.3d 430 (3d Cir. 1997).....	44, 45
<i>QVC, Inc. v. Resultly, LLC,</i> 159 F. Supp. 3d 576 (E.D. Pa. 2016)	21
<i>Red Lion Med. Safety, Inc. v. Ohmeda, Inc.,</i> 63 F. Supp. 2d 1218 (E.D. Cal. 1999).....	41
<i>Reifert v. S. Cent. Wis. MLS Corp.,</i> 450 F.3d 312 (7th Cir. 2006)	28, 36, 38
<i>Republic Tobacco Co. v. N. Atl. Trading Co.,</i> 381 F.3d 717 (7th Cir. 2004)	26, 27

<i>Rhinehart v. Scutt,</i> 2014 WL 5361936 (E.D. Mich. 2014).....	21
<i>Roland Mach. Co. v. Dresser Indus., Inc.,</i> 749 F.2d 380 (7th Cir. 1984)	26, 29
<i>Schor v. Abbott Labs.,</i> 457 F.3d 608 (7th Cir. 2006)	42, 45
<i>Thiesing v. Dentsply Int'l, Inc.,</i> 748 F. Supp. 2d 932 (E.D. Wis. 2010).....	55
<i>Times-Picayune Publ'g Co. v. United States,</i> 345 U.S. 594 (1953).....	35
<i>Todd v. Exxon Corp.,</i> 275 F.3d 191 (2d Cir. 2001).....	46
<i>Toys "R" Us, Inc. v. FTC,</i> 221 F.3d 928 (7th Cir. 2000)	20, 23, 37
<i>United States v. Brown,</i> 936 F.2d 1042 (9th Cir. 1991)	23
<i>United States v. Microsoft Corp.,</i> 253 F.3d 34 (D.C. Cir. 2001).....	27, 34
<i>United States v. Topco Assocs., Inc.,</i> 405 U.S. 596 (1972).....	24
<i>United States v. Visa U.S.A., Inc.,</i> 344 F.3d 229 (2d Cir. 2003).....	37
<i>Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP,</i> 540 U.S. 398 (2004).....	25, 47
<i>West Penn Allegheny Health Sys., Inc. v. UPMC,</i> 627 F.3d 85 (3d Cir. 2010).....	31
<i>Wilk v. Am. Med. Ass'n,</i> 895 F.2d 352 (7th Cir. 1990)	45
<i>ZF Meritor, LLC v. Eaton Corp.,</i> 696 F.3d 254 (3d Cir. 2012).....	46

<i>Zahn v. North Am. Power & Gas, LLC,</i> 815 F.3d 1082 (7th Cir. 2016)	19
---	----

STATUTES AND RULES

18 U.S.C. § 1030(a)(2)(C)	52-53
Fed. R. Civ. P. 12(b)(6).....	1, 2, 19, 20, 29
Fed. R. Evid. 801(d)(2)(D)	21
Wis. Stat. § 943.70(2)(a)(6)	52

OTHER MATERIALS

Model Jury Instructions in Civil Antitrust Cases, Instruction 3C, Rule of Reason – Evidence of Competitive Benefits.....	31
Orin Kerr, <i>Norms of Computer Trespass</i> , 116 Colum. L. Rev. 1143 (2016)	53
Restatement (Second) of Torts § 767.....	54
Restatement (Second) of Torts § 773.....	54, 55
Restatement (Third) of Agency § 1.01 (2006).....	52

INTRODUCTION

Plaintiff Authenticom, Inc. (“Authenticom”) has alleged antitrust and tortious interference claims against Defendants CDK Global, LLC (“CDK”) and The Reynolds and Reynolds Company (“Reynolds”), the two dominant providers of car dealership software systems. Authenticom’s Complaint alleges, based on direct evidence and admissions, that Defendants conspired to block Authenticom – a *per se* antitrust violation – and have inflicted harm on consumers through contractual restraints and exclusionary conduct. This Court has already found Authenticom’s horizontal conspiracy and exclusive dealing claims meet the likelihood-of-success standard for a preliminary injunction, a standard more demanding than that which applies on a Rule 12(b)(6) motion. *See* Opinion & Order (Dkt. 172) (“Op.”). Defendants’ motions to dismiss should be denied.

First, Authenticom’s allegations of horizontal conspiracy satisfy the standard of plausibility required under *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007). Defendants’ executives told Authenticom’s founder and CEO Steve Cottrell that CDK and Reynolds had agreed to block Authenticom’s access to dealer data in order to drive it out of business, and CDK and Reynolds committed to writing an agreement halting competition and dividing the data integration market between themselves. That is direct evidence of conspiracy, which renders unnecessary any resort to an inference of conspiracy based on circumstantial evidence. Defendants argue Mr. Cottrell’s account is implausible, but courts do not make such credibility determinations on a motion to dismiss (allegations in the Complaint must, of course, be taken as true).

Moreover, the February 2015 agreements not only corroborate the existence of Defendants’ conspiracy to drive Authenticom out of business, those agreements – standing alone – constitute *per se* unlawful market division. In those agreements, CDK agreed to end its data

integration business on the Reynolds platform and steer its customers to Reynolds, replacing competition with cooperation. And, just as significant, Defendants agreed not to access each other's DMS systems – which they labeled a “contractual restriction on access” – and agreed to help each other lock out third-party integrators. This Court found the February 2015 agreements “essentially have th[e] effect” of blocking third-party integrators like Authenticom. Op. 8.

Second, Authenticom has plausibly alleged Defendants' vertical restraints with vendors and with dealers have substantially foreclosed Authenticom from the market and are unlawful under the rule of reason (in the case of the exclusive dealing arrangements) or *per se* (in the case of the alleged tying arrangements). *See* Op. 15 (finding a likelihood that Authenticom could show that Defendants' agreements with vendors are unlawful exclusive dealing arrangements). Authenticom has alleged Defendants have raised prices well above competitive levels: whereas Authenticom charges around \$50 a month for data integration, CDK and Reynolds charge \$700 or more for the same services. Defendants' conduct and price increases have reduced output, forcing vendors to shutter applications and dealers to forego applications they would otherwise purchase.

Defendants' argument that these competitive harms are justified by pro-competitive benefits raises a factual issue not appropriate to resolve on a Rule 12(b)(6) motion and, in any event, is belied by the Complaint and the evidence adduced consistent with the Complaint. In particular, Authenticom alleges in detail why Defendants' proposed security and system concerns are largely pretextual. And, based upon the evidence adduced at the preliminary injunction hearing, this Court likewise concluded Defendants' security-based rationales – while “plausible” in theory – were not supported by the evidence, given Defendants' own course of

conduct and Authenticom's unblemished security record over 15 years in the industry. Op. 4, 19.

Third, Authenticom has alleged claims of unlawful monopolization under Section 2 of the Sherman Act. Authenticom has plausibly alleged that high switching and information costs prevent dealers from easily switching between DMS brands – market conditions that have allowed Defendants to exploit dealers' sunk costs and charge monopoly prices for data integration on the respective CDK and Reynolds DMS platforms. *See Eastman Kodak Co. v. Image Tech. Servs.*, 504 U.S. 451 (1992). And, Authenticom has alleged Defendants have acquired and maintained their aftermarket monopolies through exclusionary and anti-competitive tactics targeting both competitors and consumers – not just (as Defendants incorrectly suggest) a refusal to cooperate or deal with Authenticom itself.

Fourth, contrary to Reynolds' assertions, the Computer Fraud and Abuse Act ("CFAA") is irrelevant to Authenticom's antitrust claims. The Supreme Court long ago rejected any "illegality" defense to private antitrust lawsuits. Moreover, the CFAA is not an antitrust immunity statute: if CDK and Reynolds violated Section 1 of the Sherman Act by agreeing to block Authenticom's access – or if, acting unilaterally, they unlawfully prevented dealers from providing automated access to their own operational and business data – the CFAA does not affect Authenticom's antitrust challenge. In any event, Authenticom's access to dealer data was not "without authorization" or "exceeding authorized access" under the CFAA because the access was authorized by dealers – who own the data (as Defendants admit).

Fifth, Authenticom has plausibly alleged tortious interference under Wisconsin law because Defendants have intentionally interfered with Authenticom's business relationships with vendors and dealers. Defendants' claims that their interference was justified raises a factual

defense that is not appropriate to resolve on a motion to dismiss. In any event, there is no legally protected interest in violating the antitrust laws, rendering Defendants' interference without justification.

FACTUAL BACKGROUND¹

I. Parties and Industry Background

1. CDK and Reynolds are the nation's dominant providers of DMS software, controlling three quarters of the market by number of dealers. Compl. ¶ 3. There are approximately 18,000 franchised car dealerships in the United States, Dkt. 164 (89:10-11), and each relies on a DMS as "mission-critical software that enables dealerships to run their operations and function as a business," Compl. ¶ 28. Combined, CDK and Reynolds control 72% of the DMS market, with CDK controlling 42% and Reynolds 30%. Op. 3; Dkt. 127, ¶ 7; Dkt. 97, ¶¶ 8, 10; Compl. ¶ 33. There are smaller, niche DMS providers, but for most dealers, "CDK or Reynolds are your only choices. They own the market." Dkt. 165 (18:3-4); Compl. ¶¶ 35-36.

Car dealers use DMS software to manage critical aspects of their business, such as sales, financing, inventory management, service and repairs, payroll, and marketing. Compl. ¶ 28. The DMS includes a database component where dealers input and store customer, vehicle, parts, and inventory data created from the sales and servicing of vehicles. *Id.* ¶ 29; Dkt. 164 (85:13-20). This dealer-generated data is owned by the dealers, and not the DMS companies. Compl. ¶ 29.

¹ As explained below, *see infra* p. 19, because plaintiff may properly "elaborate on . . . factual allegations" in the Complaint "so long as the new elaborations are consistent with the pleadings," *Geinosky v. City of Chicago*, 675 F.3d 743, 745 n.1 (7th Cir. 2012), it is appropriate for the Court to consider, in addition to the Complaint's allegations, the evidence presented in the proceedings on Authenticom's motion for preliminary injunction as reflected here.

Once a dealer builds its operations on a particular DMS platform – and trains its workforce – it is disruptive and expensive to switch, as doing so “changes nearly every process that a dealer uses to operate.” Dkt. 56 (Maas Decl. ¶ 7); Dkt. 53 (Fitkin Decl. ¶ 3); Dkt. 54 (Korp Decl. ¶¶ 19-20); Compl. ¶¶ 40-45. Even changing product offerings within the same DMS company “is very difficult and time consuming.” Dkt. 54 (Korp Decl. ¶ 20). As a result of long-term contracts and high switching costs, the *average* DMS client tenure is more than 20 years. Dkt. 146, ¶ 15; Dkt. 53 (Fitkin Decl. ¶¶ 2-3); Compl. ¶ 40. The Complaint details how even some of the nation’s largest and most sophisticated car dealerships have tried and failed to switch DMS providers, highlighting Hendrick Automotive Group’s since-abandoned attempt to switch from Reynolds to CDK in mid-2016 as one example. Compl. ¶ 42.

CDK’s and Reynolds’ DMS software “is expensive.” Op. 3. A single dealership pays \$120,000 or more per year for its DMS license. *Id.*; Dkt. 55 (Longpre Decl. ¶¶ 4, 11); Dkt. 54 (Korp. Decl. ¶ 24); Compl. ¶ 37. And “[e]very year, the DMS charges go up” by contractual mandate; the increases “are never lower than 5 percent.” Dkt. 54 (Korp Decl. ¶ 24); Dkt. 55 (Longpre Decl. ¶ 11); Compl. ¶¶ 224-225.

2. Car dealers depend on software-based services, or “applications,” provided by third-party vendors, for features and essential services that are not built into the DMS. Compl. ¶ 47. Vendors require access to dealer data stored on the DMS and cannot perform services without such access. *Id.* Vendors and dealers rely on data integrators to provide vendors with the specific data required for their applications. *Id.* Data integrators specialize in pulling dealer data from the DMS, organizing it into a standardized format free of data-entry errors, and delivering the data in an automated way without the need for dealers to manually intervene. *Id.*; Dkt. 164 (87:11-20).

There is no dispute that the data relevant to this lawsuit belongs to the dealer. Compl. ¶¶ 64-67; Op. 3 (“The data itself belongs to the dealer.”); Dkt. 56 (Maas Decl. ¶¶ 8-9); Dkt. 55 (Longpre Decl. ¶ 4); Dkt. 53 (Fitkin Decl. ¶ 4). Reynolds’ website represents to dealers: “Your Data, Your Way. You own your data. Reynolds recognizes you need to share that data outside your dealership.” Compl. ¶ 65. CDK’s website likewise states: “[D]ealerships own their data.” *Id.* ¶ 66; *see also id.* (CDK “has always understood that dealerships own their data.”). Defendants’ DMS contracts with dealers likewise recognize dealers’ ownership of the data. *Id.* ¶ 67.

CDK, in particular, has repeatedly made public statements affirming the principle that dealerships own the data that they store on the DMS. Compl. ¶¶ 68-71. As CDK’s longtime CEO Steve Anenen told *Automotive News*, dealers have the right to grant third parties such as data integrators access to their data, and CDK was “not going to prohibit that or get in the way of that.” *Id.* ¶ 69. Mr. Anenen explained, “I don’t know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it, when in fact it’s really the data belonging to the dealer. As long as they grant permission, how would you ever go against that wish?” *Id.*

3. Authenticom is a data integrator that was founded in 2002 by Steve Cottrell in La Crosse, Wisconsin. Compl. ¶ 77. Before Defendants implemented their anticompetitive agreement, Authenticom was an American success story, growing from a single employee in 2002 to 120 employees in 2015. *Id.* President Barack Obama singled out Authenticom – in a July 2, 2015 speech in La Crosse – as “one of America’s fastest growing private companies” that had succeeded through innovation and dedication to its customers and employees. *Id.* Out of

18,000 dealerships nationwide, over 15,000 have used Authenticom. Op. 4; *see also* Dkt. 164 (89:7-11); Compl. ¶ 13.

Authenticom’s primary product is DealerVault, “which gives dealers state-of-the-art control over how their data is pulled and shared. It provides a unified user interface where dealers, with the click of a button, are able to add, remove, or change the data sets that Authenticom pulls from the DMS.” Compl. ¶ 78. DealerVault has been well received by dealers; Wayne Fitkin, an IT director for a California dealership, testified that DealerVault is an “incredibly exceptional product” and the “best thing I have seen” in 30 years in the industry; and Brian Maas, the president of the California New Car Dealers Association, testified that DealerVault is the “best product in its market space.” Dkt. 165 (6:13-24); Dkt. 162 (183:14-21); Compl. ¶ 77. As this Court found after hearing testimony regarding DealerVault at the preliminary injunction hearing, DealerVault “has already won acceptance in the market” and “is popular with dealers, who generally feel strongly that because they own their data, they should be able to control and monitor its use.” Op. 4, 20.

Authenticom always obtains express authorization from the dealer before pulling dealer data from the DMS on behalf of the dealer. Compl. ¶ 55; Dkt. 164 (108:4-13); *see id.* (91:3-9) (Mr. Cottrell testifying that the key terms in Authenticom’s contracts with dealers provide that Authenticom may “only access the data that the dealer expressly provides [Authenticom] permission for,” and Authenticom may “only transmit the data to the vendors that the dealer expressly gives [Authenticom] permission to through their contracts between the dealers and the vendors”); Dkt. 65-3 (contract between dealer and Authenticom). Authenticom “cannot and would not” pull dealer data without the dealer’s explicit authorization. Dkt. 164 (103:19-21).

Authenticom's "security practices are state of the art" and Authenticom has an unblemished security record. Compl. ¶¶ 84-85; Op. 4 (The evidence "shows that Authenticom is secure."). DealerVault is hosted "on Microsoft Azure, secure cloud technology." Op. 4. In its 15-year history, Authenticom has never had a data breach; its firewall has never been compromised; and it has never had a reportable security incident. Op. 5; Dkt. 164 (114:12-17); Compl. ¶ 84. If a data security event ever were to happen, Authenticom has a \$20 million cyber-liability insurance policy. Compl. ¶ 85; Dkt. 62 (Cottrell Decl. ¶ 32).

CDK and Reynolds also provide data integration services as products separate from the core DMS, which compete with Authenticom. CDK owns two of the largest data integrators in the industry, DMI and IntegraLink, which, like Authenticom, obtain dealers' authorization and dealer login credentials to provide data integration services. Compl. ¶ 88; *see* Dkt. 163 (69:12-14) (Robert Schaefer of Reynolds testifying that Reynolds still allows CDK to use usernames and passwords to pull data from Reynolds dealers). DMI and IntegraLink provide data integration services for dealers using non-CDK DMS systems; CDK also provides access to dealer data on the CDK DMS through its own data integration product called the Third Party Access, or 3PA program. Compl. ¶¶ 89-90, 95-101. Reynolds provides its own data integration product, the Reynolds Certified Interface, or RCI program, for access to dealer data on the Reynolds DMS. *Id.* ¶ 102.

4. For over a decade, CDK and Reynolds did not interfere with dealers' use of independent data integrators. Compl. ¶ 5. Competition in the data integration market flourished, with numerous providers (including Authenticom) competing for the business of dealers and vendors. Compl. ¶¶ 106-110. Reynolds first began blocking dealer-authorized independent data integration in 2009, followed by "more effective blocking" around 2013. Op. 5. "In June 2013,

Reynolds intensified its tactics by disabling Authenticom’s usernames en masse,” which was accompanied by a public announcement to its dealer-customers that Reynolds “will begin the rollout of prohibiting automated access” into its DMS. Compl. ¶ 189.

During this time, CDK continued to allow the use of independent data integrators until August 2015. *Id.* ¶ 7. For years, CDK touted its open system as a competitive advantage of its DMS over Reynolds’ DMS. *Id.* ¶ 6.

II. The Horizontal Conspiracy Between CDK and Reynolds

As the Complaint alleges, CDK made an about-face in 2015, repudiated its longstanding public position, and switched to a “closed” system. Compl. ¶¶ 7-8, 94, 189. Consistent with these allegations, [REDACTED]

[REDACTED] Op. 6 (“CDK realized that it was not getting all the value it could from 3PA, its third-party access program.”); Dkt. 163 (132:20-133:2) (CDK executive, Malcolm Thorne, admitting that “part of the rationale for the 3PA refresh was a profit motive for CDK”).

CDK recognized that competition from third-party integrators like Authenticom posed a direct threat to its ability to raise the prices it charges vendors for data integration: an internal CDK presentation noted [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In addition to being able to raise prices, CDK believed that blocking independent integrators would [REDACTED]

■ By controlling the flow of data from its DMS customers, CDK intended to place competing application providers at a disadvantage. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

CDK's internal documents also acknowledge that it wanted Reynolds' cooperation in eliminating independent integrators. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

A few months later, in early 2015, CDK and Reynolds entered into agreements designed to eliminate competition in the provision of dealer data integration services. Compl. ¶¶ 7-8, 117-130; *see also* Op. 6-8; Dkt. 106-1, Dkt. 106-2, Dkt. 106-3. First, in February 2015, Defendants entered into three written agreements in which they promised not to compete in providing data integration services and, in their capacity as application providers, not to use the services of independent integration service providers to obtain data from the other's DMS. Op. 6-7. Second, CDK and Reynolds further agreed that each would block independent integrators' access to their DMS customers' data in an effort to drive independent integrators from the market entirely. Op. 8, 12; Dkt. 62 (Cottrell Decl. ¶¶ 48-52); Dkt. 164 (139:6-143:24) (Cottrell testimony); Compl. ¶ 179-181.

1. February 2015 Agreements. Pursuant to the February 2015 written agreements, CDK agreed that it would no longer compete with Reynolds' own RCI integration product in providing access to dealer data on the Reynolds DMS. Compl. ¶ 132; *see* Dkt. 106-1 (Wind-Down Access Agreement). CDK also agreed to cooperate with Reynolds in transferring CDK's vendor customers to Reynolds. *See* Compl. ¶¶ 133, 136-138; Dkt. 106-1; Dkt. 163 (71:8-25). Reynolds, in return, gave CDK a five-year grace period in which Reynolds promised not to block CDK's access to the Reynolds DMS. *See* Dkt. 106-1; Dkt. 163 (68:21-23); *id.* (74:13-18); *see also* Compl. ¶ 141.

CDK and Reynolds also agreed that they themselves would no longer access data on each other's DMSs. Dkt. 163 (agreeing to “[p]rohibition on . . . DMS Access”). Specifically, the agreement states: “For the avoidance of doubt, this Section 4.5 is not intended as a ‘covenant not to compete,’ but rather as a contractual restriction of access and attempted access.” *Id.* This restriction lasts forever. Dkt. 106-1, § 6.1; Op. 7 (“Section 4.5’s terms do not expire.”). Defendants’ witnesses confirmed that Section 4.5 prohibits them from accessing each other’s DMSs. Robert Schaefer, Reynolds’ Vice President of Data Services, testified: “Q: In this contract by its plain term Section 4.5, Reynolds agreed not to access the CDK DMS; isn’t that right? A: That would be correct.” Dkt. 163 (76:6-9). The testimony is the same with respect to CDK’s prohibition on access of the Reynolds DMS. *Id.* (73:11-16, 75:16-76:1) (Schaefer testimony). In two supplemental agreements, Defendants, in their capacities as application providers, agreed that they would use each other’s in-house integration products, RCI and 3PA. Dkts. 106-2, 106-3 (CDK agreed to purchase data integration through RCI, and Reynolds received five years of free data integration using 3PA).

The market division agreement directly harmed Authenticom. Compl. ¶ 148. During the “wind-down” period, Authenticom lost many customers to CDK’s affiliate, Digital Motorworks. *Id.*; *see also* Dkt. 164 (137:4-18); Dkt. 62 (Cottrell Decl. ¶ 58). Vendors decided to leave Authenticom (which Reynolds was actively blocking) and to join CDK (which was not being blocked) on an interim basis, even if those vendors knew they would ultimately be forced into the RCI program. Compl. ¶ 148; Dkt. 62 (Cottrell Decl. ¶ 58); Dkt. 165 (31:1-32:15) (Andreu testimony) (“We switched [from Authenticom] to DMI” during “CDK’s grace period or safe haven or wind down.”). CDK and Reynolds thus cooperated in driving vendors away from Authenticom.

2. Conspiracy To Eliminate Authenticom. In granting Authenticom’s motion for a preliminary injunction, this Court explained that “the February 2015 agreements . . . suggest a horizontal conspiracy” because, “[a]lthough the agreements do not explicitly state that defendants will work together to eliminate third-party data integrators, the agreements have that effect.” Op. 12. In addition to Defendants’ written agreements, senior CDK and Reynolds executives also have admitted to Authenticom’s founder and CEO, Mr. Cottrell, that Defendants have agreed to restrict access to dealer data and destroy data integrators like Authenticom. Compl. ¶¶ 179-181; Op. 8, 12.

As the Complaint alleges – and Mr. Cottrell testified at the preliminary injunction hearing – Reynolds’ Mr. Schaefer told Mr. Cottrell that Reynolds had “made agreements with the other major DMS providers” – there is only CDK – “to support each other’s third-party access agreements *and* to block independent integrators such as Authenticom.” Compl. ¶ 181; Dkt. 164 (139:6-13) (emphasis added). Mr. Schaefer said that Reynolds’ owner, Bob Brockman, “was adamant” that all third-party data integrators must be cut off. Compl. ¶ 181. As a result, Mr.

Schaefer said that Authenticom should wind down its operations and leave the market. Dkt. 164 (138:3-139:19); *see also* Compl. ¶ 181.

A top executive at CDK delivered the same message to Mr. Cottrell. Compl. ¶ 180; Dkt. 164 (140:1-143:1); Dkt. 62 (Cottrell Decl. ¶¶ 48-51). On April 3, 2016, at an industry convention in Las Vegas, Dan McCray (CDK's former Vice President of Product Management) stopped by Authenticom's booth to talk with Mr. Cottrell, who was occupied with a customer. Dkt. 164 (140:1-143:1). After Mr. Cottrell finished with the customer, he walked to CDK's booth, where he saw Mr. McCray "standing off to the side" with "three other individuals." *Id.* After cordial greetings, Mr. McCray took Mr. Cottrell by the arm and said, "[l]et's take a walk." *Id.*; Compl. ¶ 180. Mr. McCray led Mr. Cottrell off the convention floor and down a service ramp to a secluded area. Dkt. 164 (140:1-143:1). Mr. McCray then confirmed the existence of the illegal agreement, stating that CDK and Reynolds had agreed to "lock you and the other third parties out," and that they were "working collaboratively to remove all hostile integrators from our DMS system." *Id.*; *see* Compl. ¶ 180. Mr. McCray then grew threatening: "I wanted to look you in the eye and let you know man to man, I have been mandated by our new CEO to seek you out and destroy your business on our systems." Compl. ¶ 180; Dkt. 62 (Cottrell Decl. ¶ 49). "For god's sake," he concluded, "you have built a great little business, get something for it before it is destroyed otherwise I will f***ing destroy it." Compl. ¶ 180; Dkt. 62 (Cottrell Decl. ¶ 50); Dkt. 164 (142:9-12). Mr. Cottrell rejected Mr. McCray's threats and insisted that Authenticom would continue to serve its dealer and vendor customers. Compl. ¶ 180; Dkt. 62 (Cottrell Decl. ¶ 51). After a sleepless night, Mr. Cottrell got up the next morning and memorialized the details of what Mr. McCray had said. *See* Dkt. 66-05; PHX-055A; Dkt. 66-6 (metadata for notes).

At the preliminary injunction hearing, this Court “credit[ed] Cottrell’s testimony” as to these events as “more persuasive” than the conclusory denials of Mr. Schaefer and Mr. McCray. Op. 12.

III. Restrictive Vertical Agreements

Defendants have imposed restrictive agreements in both dealer and vendor contracts. These provisions require dealers to agree, as a condition of obtaining DMS service, that they will not provide access to their data to anyone else, and vendors to agree, as a condition of obtaining data integration services from CDK or Reynolds, that they will not obtain such services from anyone else for *any* CDK or Reynolds dealer respectively. Compl. ¶¶ 149-165.

Vendors. For a vendor to use 3PA for *any* of its dealer customers on the CDK platform, the vendor must agree to use 3PA exclusively for *all* of its dealer customers on the CDK platform. *See* Compl. ¶¶ 159-162; [REDACTED] [REDACTED]; Dkt. 163 (177:8-12) (same). The same is true for RCI and Reynolds’ DMS customers. *See* Compl. ¶¶ 163-165; [REDACTED]

CDK’s Vice President of Data Services and the head of the 3PA program, Howard Gardner, conceded that the exclusive dealing provision requiring vendors to obtain dealer data exclusively through the 3PA program lasts forever because it “survive[s] the termination of this agreement.” Dkt. 163 (179:9-20); *see also* Compl. ¶ 161.

CDK and Reynolds also impose price secrecy provisions in their 3PA and RCI contracts prohibiting vendors from informing dealers about the data access fees, whether directly or indirectly, even though the data access fees are passed down to dealers in the form of higher vendor prices. Compl. ¶¶ 166-170; Dkt. 106-39, § 8 (CDK); Dkt. 66-3, §§ 2.5.3, 2.7 (Reynolds). For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Compl. ¶ 168; Dkt. 106-39, § 8; *see also* Compl. ¶ 169 (parallel Reynolds term).

Dealers. “In their DMS contracts with dealers, both CDK and Reynolds require dealers to agree that they will not provide anyone other than the DMS provider access to their data for purposes of data integration and syndication to vendors. The contractual terms thus prohibit dealers from granting access to their data to anyone else, including data integrators such as Authenticom.” Compl. ¶ 150; *see also id.* ¶¶ 151-152. Reynolds prohibits dealers from “provid[ing] access to [the DMS database] . . . to any third party,” while granting Reynolds the sole right [REDACTED] Compl. ¶ 152; Dkt. 65-24, § 1; Dkt. 64-17.

CDK’s standard DMS contract, on the other hand, has long stated that a dealer’s “employees *and agents*” may “have access” to the DMS, but that dealers “shall not allow access to [the CDK DMS database]” to anyone else. Dkt. 106-10, § 6.D. CDK now takes the position that this language prohibits independent integrators from accessing dealer data – and that only CDK may provide integration services to a dealer – even though CDK took the opposite position for decades before it entered into the agreement with Reynolds. *See* Compl. ¶¶ 66, 69-71, 155. CDK and Reynolds vigilantly enforce the restrictive terms in their DMS contracts by disabling the login credentials dealers provide to independent integrators. Compl. ¶¶ 153-156; Op. 5-6.

IV. Harm to Competition

The Complaint alleges that – through their horizontal and vertical restraints – CDK and Reynolds have been able to eliminate competition, raise prices above competitive levels, and reduce output. Compl. ¶¶ 153-156

Price Increases. Authenticom has alleged – and presented extensive evidence to support – that CDK and Reynolds have imposed massive price increase on dealers and vendor for data integration services, raising prices far above competitive levels. As the Complaint alleges, Authenticom charges \$25 to \$50 for data integration services on a per-month, per-dealership basis. Compl. ¶ 214. Other independent integrators – before being forced out of the market by Defendants – charged similar rates. *Id.* Defendants, however, charge massively higher monthly rates (exceeding \$700), in addition to an array of up-front and add-on fees that independent integrators do not charge. *Id.* ¶¶ 215-216. CDK and Reynolds also have each sharply increased the rates they charge compared to their prices from a few years ago, before they eliminated competition on their platforms. *Id.* ¶¶ 217-220.

Consistent with these allegations, Authenticom produced unrebutted evidence at the preliminary injunction hearing – from both vendors and dealers – of huge and harmful price increases. Mr. Alan Andreu of the vendor Dominion Enterprises (“Dominion”) testified that after Reynolds’ blocking forced application vendor Dominion into the RCI program in 2011, the initial cost was “\$247 [a month] compared to the \$30 [Dominion] w[as] paying” Authenticom. Dkt. 165 (30:24-25). Reynolds has since raised its price from \$247 to \$893, compared to the \$30 to \$50 that Authenticom has consistently charged. *Id.* (32:18-24). Mr. Andreu testified that CDK charges \$457 a month, which is “cheap” compared to Reynolds, “until you compare it to that \$30 that [Dominion] could have paid Authenticom.” *Id.* (39:1-3). Likewise, Matthew Rodeghero of vendor AutoLoop testified that Reynolds and CDK charge \$905 and \$690, respectively, for the same services that independent data integrators provide for a fraction of the price. Dkt. 165 (69:11-18); *id.* (59:5-62:15). Dealers ultimately bear the brunt of these high costs, as vendors generally pass along all or most of Defendants’ data integration fees. Dkt. 162

(198:13-199:3); Dkt. 165 (14:1-20); *see* Compl. ¶¶ 224, 228, 229. These increased costs to dealers are not offset by reductions in DMS prices. Compl. ¶ 130.

Reduced Output. Defendants’ elimination of competition in the data integration market has also reduced output by limiting customer choice and reducing innovation and the availability and quality of applications. Compl. ¶¶ 226-31. Consistent with these allegations, Mr. Andreu of Dominion testified at the preliminary injunction hearing that Dominion shuttered one product because of Reynolds’ data integration fees. Dkt. 165 (35:11-20); Dkt. 165 (44:15-45:3) (Andreu testimony). Michael Korp, owner of Chicago-based vendor Open Recalls – which helps dealerships track down car owners with unresolved safety recalls – testified that he could not afford Defendants’ high integration fees, and therefore will go out of business if he can no longer use Authenticom. Dkt. 162 (191:14-195:8). Dealers likewise cannot use the applications they otherwise would because those large fees are passed down to them. *See, e.g.*, Dkt. 53 (Fitkin Decl. ¶ 20); Dkt. 54 (Korp Decl. ¶ 31) (“[T]he data access fees CDK charges are so high” that they “make the passed-through fees cost-prohibitive.”).

V. Authenticom Does Not Compromise Defendants’ Data Security or System Integrity

At the preliminary injunction hearing, this Court rejected Defendants’ attempts to justify their anticompetitive actions on the basis of ensuring data security and system integrity. Op. 15-16; *see also* Compl. ¶¶ 234-241. The Court explained that even though Defendants “presented evidence that they had invested vast sums in their respective DMSs,” they “did not put in any evidence to quantify the additional expense of providing data integration services.” Op. 15. The Court was “not convinced that Authenticom’s access [to Defendants’ DMS systems] poses significant risks,” noting that Reynolds, for example, “already allows many exceptions to its ‘no hostile integration’ policy.” *Id.* at 18-19. Authenticom presented evidence that Reynolds has “whitelisted,” or protected Authenticom usernames and passwords, for Penske Automotive

Group, the largest auto group in the nation, as well as for Jaguar and BMW, among others. *See* Dkt. 164 (127:5-129:14, 133:14-22); Dkt. 163 (43:20-23, 86:12-88:8); Dkt. 147-14; Dkt. 147-21; Dkt. 164 (129:15-132:15, 133:14-22); PHX-159. Reynolds has also whitelisted a large number of usernames and passwords for CDK so that CDK can continue screen scraping data from the Reynolds DMS during the five-year “wind down” period pursuant to Defendants’ February 2015 agreement. Dkt. 163 (36:6-37:13, 69:15-70:16, 73:22-74:6); *see* Compl. ¶¶ 140, 232.

As the Court observed, “[t]he evidence generally shows that Authenticom is secure,” as DealerVault is hosted on secure cloud technology and has never suffered a security breach, and “the data to which Authenticom has access is controlled by the dealer.” Op. 4; *see* Dkt. 165 (9:12-21) (Fitkin testimony). The Court further found that there is no evidence that “Authenticom’s access to defendants’ DMS imposes a substantial burden,” as Defendants failed to “submit evidence that would allow the court to determine what proportion of overall system resources were expended on Authenticom’s queries [to the DMS],” as well as “evidence to show how much more resources Authenticom’s queries consumed than would have been consumed if the dealers and vendors had used some other, approved means of accessing data.” Op. at 19.

VI. Harm to Authenticom

As the Complaint alleges, “Defendants’ anticompetitive conduct has nearly destroyed the entirety of Authenticom’s business.” Compl. ¶ 233; Op. 16-17 (Defendants’ conduct has brought Authenticom’s business to “the brink of collapse.”). Defendants’ joint blocking of Authenticom has been “devastating to [its] relationship with . . . [its] vendor partners and dealers,” and resulted in numerous cancellations. Dkt. 164 (146:15-16); Dkt. 66-15 (cancelling “with reluctance” and as “solely the result of CDK’s aggressive” blocking of Authenticom; “[b]eing forced to do business with CDK is distressing.”); Dkt. 66-16 (similar); *see* Compl. ¶ 209. As a result, as this Court found, Authenticom has suffered a “dramatic drop-off in

revenue,” has “very limited cash reserves,” and has breached a covenant “with its lender on a substantial loan.” Op. 16-17.

ARGUMENT

In resolving Defendants’ Rule 12(b)(6) motion, the Court must assume the truth of the factual allegations in Authenticom’s Complaint, drawing all reasonable inferences in Authenticom’s favor. *See Zahn v. North Am. Power & Gas, LLC*, 815 F.3d 1082, 1087 (7th Cir. 2016). The Court considers, in addition to the allegations in the Complaint, “‘documents attached to the complaint, documents that are critical to the complaint and referred to in it, and information that is subject to proper judicial notice,’” along with additional facts set forth in Authenticom’s brief opposing dismissal, so long as those additional facts “‘are consistent with the pleadings.’” *Phillips v. Prudential Ins. Co. of Am.*, 714 F.3d 1017, 1020 (7th Cir. 2013) (“We also must consider additional facts set forth in Phillips’s district court brief and appellate briefs, so long as those facts ‘are consistent with the pleadings.’”) (quoting *Geinosky*, 675 F.3d at 745 n.1). Thus, plaintiff “may elaborate on his factual allegations so long as the new elaborations are consistent with the pleadings.” *Geinosky*, 675 F.3d at 745 n.1 (collecting cases). The Court may therefore properly consider the evidence from the preliminary injunction hearing, as set forth in this opposition, in evaluating whether Authenticom has stated a claim for relief.

I. Authenticom Has Stated Plausible Claims Under Section 1 of the Sherman Act

A. The Complaint Alleges a Per Se Unlawful Horizontal Conspiracy

1. Defendants Agreed To Block Independent Integrators and Drive Them from the Market

1. The Complaint adequately pleads an unlawful horizontal conspiracy in violation of Section 1 of the Sherman Act. The Complaint alleges that executives from both CDK and Reynolds told Authenticom’s Mr. Cottrell that Defendants were working together to block

Authenticom's access to dealer data so it could no longer compete. *See supra* pp. 12-14; *see also* Compl. ¶¶ 10, 180, 181, 185. This Court has already credited Mr. Cottrell's "detailed" and "persuasive" testimony at the preliminary injunction stage. Op. 12. Specific, credible allegations of an admitted conspiracy far exceeds the Rule 12(b)(6) plausibility threshold: it is, on its own, "all the proof" that Authenticom needs to prove its claim at trial, let alone survive a motion to dismiss. *In re High Fructose Corn Syrup Antitrust Litig.*, 295 F.3d 651, 654 (7th Cir. 2002).

Defendants have never argued that an agreement between horizontal competitors to block rivals' access to their respective DMSs is lawful, nor could they. "[J]oint efforts by a firm or firms to disadvantage competitors by . . . persuading or coercing suppliers or customers to deny relationships the competitors need in the competitive struggle" are *per se* unlawful. *Toys "R" Us, Inc. v. FTC*, 221 F.3d 928, 936 (7th Cir. 2000) (quoting *Nw. Wholesale Stationers, Inc. v. Pac. Stationery & Printing Co.*, 472 U.S. 284, 294 (1985)); *see also Klor's, Inc. v. Broadway-Hale Stores, Inc.*, 359 U.S. 207, 212 (1959).

Furthermore, Defendants' emphasis on alleged concerns about data security and system performance do not provide even a potential defense with respect to this claim. A *per se* unlawful agreement cannot be "saved by allegations that [it was] reasonable in the specific circumstances." *Klor's*, 359 U.S. at 212. Comparable claims about "risk to public safety and health" from unregulated competition did not provide any potential justification for a horizontal restraint on price competition in *National Society of Professional Engineers v. United States*, 435 U.S. 679, 693-94 (1978). They provide no potential justification here.

In granting a preliminary injunction, this Court found that Authenticom has "adduced evidence that could establish the existence of a *per se* illegal horizontal conspiracy" – namely, an

agreement between CDK and Reynolds “to drive Authenticom from the market,” just as the Complaint alleges. Op. 12. Accordingly, Authenticom has already established a likelihood of success “*on the merits*” of its Section 1 claim for horizontal conspiracy. *Girl Scouts of Manitou Council, Inc. v. Girl Scouts of U.S. of Am., Inc.*, 549 F.3d 1079, 1096 (7th Cir. 2008) (emphasis added). As courts have observed, “the standard for obtaining injunctive relief is considerably higher than the standard for surviving dismissal [under Rule 12(b)(6)].” *Jurista v. Amerinox Processing, Inc.*, 492 B.R. 707, 778 (D. N.J. 2013); *see QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 594 n.6 (E.D. Pa. 2016) (same); *Rhinehart v. Scutt*, 2014 WL 5361936, at *11 (E.D. Mich. June 20, 2014) (same). Where, as here, Authenticom has established “at least a moderate chance of success” on the merits, Op. 1, it has necessarily established that its claims are plausible on their face.²

2. Defendants’ assertion (CDK Br. 10-13; Reynolds Br. 24-27) that there could have been no conspiracy because CDK and Reynolds did not need to agree to exclude Authenticom – each could, they argue, do so unilaterally – is unavailing. This Court has already found that Mr. Cottrell’s account was credible, not implausible. Op. 12. Defendants’ statements – which are admissible against both Defendants for the truth of the matter asserted, *see* Fed. R. Evid. 801(d)(2)(D) – provide direct evidence of an agreement. “[W]ith direct evidence the fact finder

² See, e.g., *Eli Lilly & Co. v. Arla Foods Inc.*, 2017 WL 2976697, at *2 (E.D. Wis. July 11, 2017) (denying defendant’s motion to dismiss, noting that the court already concluded at the preliminary injunction stage that plaintiff had successfully stated certain claims, and “[n]othing [plaintiff] has put forward in its motion to dismiss disturbs those conclusions”); *Motorola, Inc. v. Pick*, 2004 WL 5472092, at *3 (C.D. Cal. June 22, 2004) (denying defendant’s motion to dismiss following a grant of a preliminary injunction because plaintiff, “[h]aving met its burden on its motion for preliminary injunction, . . . easily met the less stringent burden of Rule 12(b)(6)”; *Child Evangelism Fellowship of Minn. v. Elk River Area Sch. Dist. #728*, 599 F. Supp. 2d 1136, 1141-42 (D. Minn. 2009) (explaining that plaintiff “is likely to succeed on the merits” as part of the court’s granting of a preliminary injunction and that “[defendant’s] Motion to Dismiss is, therefore, denied”).

is not required to make inferences to establish facts.” *Omnicare, Inc. v. UnitedHealth Grp., Inc.*, 629 F.3d 697, 706 (7th Cir. 2011).

Furthermore, the Complaint alleges (and the preliminary injunction hearing identified) substantial additional evidence of an explicit agreement. Internal CDK documents reveal that part of its strategy for “closing” its DMS to third-party data integrators included reaching agreements with Reynolds to ensure it would cooperate in eliminating opportunities for independent integrators. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] Moreover, contrary to Reynolds’ assertion (at 22-24), the terms of the written agreements between CDK and Reynolds – which are independently unlawful as explained below – further confirm that Defendants agreed to cooperate to eliminate independent integrators. In their “Data Exchange Agreement,” Defendants expressly agreed (in perpetuity) not to assist “any person . . . to access or integrate with the other’s party’s DMS.” Dkt. 106-1, §§ 4.5, 6.1. That agreement strongly supports the inference that Defendants discussed independent integrators’ role in the industry and reached a meeting of the minds that they should be eliminated. *See Op. 12* (“The February 2015 agreements between CDK and Reynolds also suggest a horizontal conspiracy.”).

In any case, Defendants’ claim (CDK Br. 11; Reynolds Br. 26-27) that they lacked a “rational economic motive to conspire,” *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 596 (1986), is belied by the Complaint, the subsequent evidence consistent with the Complaint, and this Court’s factual findings. When CDK competed against Reynolds for DMS customers by touting the benefits of open access prior to February 2015, Reynolds’ unilateral

blocking cost it customers and market share. *See* Op. 6 (decline from 40% to 28%); Dkt. 130 (Addanki Decl. ¶ 58) (prior to agreement “Reynolds’ increase in DMS access restrictions . . . was. [REDACTED]”); Dkt. 165 (84:13-17) (describing share shift from Reynolds to CDK); Dkt. 165 (92:17-23). But, after CDK switched to a closed system, the number of customers leaving Reynolds for CDK dropped sharply. *See* Dkt. 165 (102:21-103:21). It makes perfect sense that CDK would only take such a step with assurance from Reynolds that it would maintain its own policy of blocking independent integrators. *See* Dkt. 163 (250:1-7) (concession by Defendants’ expert that such assurance would be valuable to CDK). Moreover, once CDK committed not to compete on the basis of an open system, Reynolds was freed to move more aggressively to block independent integrators. *See* Dkt. 165 (57:21-58:2) (vendor’s testimony that Reynolds blocked independent integration service in 2015). Reaching a common understanding with regard to maintaining closed DMS systems was thus important for both Defendants.³

2. The February 2015 Agreements Unlawfully Divide the Data Integration Market Between CDK and Reynolds

1. Even on their own terms, the February 2015 written contracts constitute an unlawful agreement to divide the market for data integration services. Market division is a “classic per se antitrust violation.” *United States v. Brown*, 936 F.2d 1042, 1045 (9th Cir. 1991);

³ Defendants assert (CDK Br. 12; Reynolds Br. 27-28) – citing no law – that the Complaint fails to state a claim for “group boycott” because “there is no refusal to deal here,” as “defendants do not ‘deal’ with Authenticom.” But that conflates the distinct antitrust doctrines of group boycott and refusal to deal. A group boycott claim does not require that the defendants refuse to deal with the plaintiff. On the contrary, group boycotts often involve horizontal competitors that do not deal directly with the plaintiffs, as in the Supreme Court’s decision in *Klor’s*, 359 U.S. at 212-13 (defendant department store guilty of group boycott for inducing group of appliance suppliers to stop selling to plaintiff department store). Here, Defendants’ conduct is a textbook group boycott: “joint efforts by a firm or firms . . . to disadvantage competitors by . . . persuading or coercing suppliers or customers to deny relationships the competitors need in the competitive struggle.” *Toys “R” Us*, 221 F.3d at 936.

accord *Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic*, 152 F.3d 588, 591 (7th Cir. 1998). The Supreme Court “has reiterated time and time again that horizontal territorial limitations . . . are naked restraints of trade with no purpose except stifling of competition.” *United States v. Topco Assocs., Inc.*, 405 U.S. 596, 608 (1972) (quotations and citations omitted). Such agreements between horizontal competitors to reserve for one another segments of the market are always unlawful, regardless of whether the territory reserved for each was one in which both parties had previously competed. *Palmer v. BRG of Georgia, Inc.*, 498 U.S. 46, 49 (1990) (per curiam).

The February 2015 written contracts constitute an unlawful agreement to divide the market for data integration services. In those agreements, CDK agreed to forebear from providing data integration services on Reynolds’ DMS, and Reynolds agreed not to access CDK’s DMS. *See* Dkt. 106-1, § 4.5. That agreement never expires. *See id.* § 6.1. Although Defendants now contest (CDK Br. 7; Reynolds Br. 45) that characterization of their contracts, Reynolds’ Mr. Schaefer agreed with it in his testimony at the hearing. *See* Dkt. 163 (73:11-16); Dkt. 163 (75:16-76:9). Moreover, CDK agreed to steer its Reynolds DMS-based integration customers to Reynolds’ own integration service. *See* Dkt. 106-1, § 4.4 (“CDK agrees to reasonably assist and cooperate with Reynolds with respect to . . . the transition of [data integration] customers to the Reynolds RCI program with respect to Reynolds Dealers.”).

Before reaching agreement, CDK and Reynolds competed to provide data integration services for car dealerships that use Reynolds DMS platform. *See* Compl. ¶ 132. After the agreement, CDK agreed to shutter that business and to steer its existing customers to Reynolds. The agreement replaced competition with cooperation. That is per se unlawful. *See Gen. Leaseways, Inc. v. Nat’l Truck Leasing Ass’n*, 744 F.2d 588, 595 (7th Cir. 1984) (affirming grant

of preliminary injunction and noting that “the division of markets . . . is a per se violation of section 1 of the Sherman Act”). Indeed, such close coordination between supposed competitors reflected in the February 2015 agreement carries the unmistakable whiff of the “supreme evil of antitrust: collusion.” *Verizon Commc’ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004). Furthermore, even if the February 2015 agreements are somehow subject to rule of reason scrutiny – rather than per se condemnation – the Complaint plausibly alleges a reduction in competition between CDK and Reynolds in the wake of those agreements. *See* Compl. ¶¶ 139-147.

2. Defendants assert (CDK Br. 6; Reynolds Br. 23-26) that Reynolds had already succeeded in limiting CDK’s access to its DMS; that Reynolds wanted to “safely reduce dealer business disruption” for CDK’s customers; and that CDK decided, “as a business matter,” to cease hostile access. But none of this provides a justification for the restrictions on competition. If Reynolds was able to block CDK, it could have done so – it would have gained nothing from CDK’s agreement to stop accessing its system. *See* Dkt. 163 (75:2-6). The problem for Reynolds was that CDK could have taken advantage of Reynolds’ blocking to encourage Reynolds’ DMS customers to switch to CDK. *See* Dkt. 165 (100:2-16).

Reynolds also claims (at 24) that the agreements were intended as a “resolution to a legal dispute.” But that argument finds no support in the Complaint, which alleges that the February 2015 agreement was intended to divide the market, not settle legal claims. Compl. ¶¶ 118, 132. Moreover, at the evidentiary hearing, Defendants failed to adduce any evidence that Reynolds had threatened CDK with litigation, such as with a cease-and-desist letter. The February 2015 agreements themselves contain no release and no reference to potential or asserted legal claims. In any event, whatever Defendants call it, the February 2015 agreement is not immune from the

antitrust laws. *See Premier Elec. Constr. Co. v. Nat'l Elec. Contractors Ass'n, Inc.*, 814 F.2d 358, 376 (7th Cir. 1987) (“[w]hen private parties help themselves to a reduction in competition, the antitrust laws apply”); *Andrx Pharm., Inc. v. Biovail Corp. Int'l*, 256 F.3d 799, 818-19 (D.C. Cir. 2001) (private settlement not immune from antitrust laws); *Am. Needle, Inc. v. NFL* 560 U.S. 183, 193 (2010) (“[T]he Sherman Act . . . is aimed at substance rather than form.”).

Finally, Defendants also assert (CDK Br. 10-11; Reynolds Br. 27-28) that, because Reynolds had never previously offered data integration services to CDK dealers, its reciprocal agreement not to begin doing so cannot constitute a market division agreement. But an agreement by a competitor to refrain from entering a market is just as illegal as agreeing to leave the market is. *See Palmer*, 498 U.S. at 49-50 (“Each agreed not to compete in the other’s territories. Such agreements are anticompetitive regardless of whether the parties split a market within which both do business or whether they merely reserve one market for one and another for the other.”).

B. The Complaint Alleges Unlawful Exclusive Dealing

The Complaint plausibly alleges that Defendants impose anticompetitive exclusive dealing arrangements on their customers – application vendors and dealers. *See supra* pp. 14-15 (describing exclusive dealing restrictions). To the extent those agreements are purely vertical in nature, they are examined under the rule of reason. *See Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 393-94 (7th Cir. 1984). A rule-of-reason exclusive dealing claim has two elements: (1) the exclusive dealing must “foreclose competition in a substantial share of the line of commerce at issue,” *Republic Tobacco Co. v. N. Atl. Trading Co.*, 381 F.3d 717, 738 (7th Cir. 2004), such that “at least one significant competitor of the defendant” is excluded “from doing business in a relevant market,” *Roland Mach.*, 749 F.2d at 394; and (2) “the probable (not

certain) effect of the exclusion” must be to “raise prices above (and therefore reduce output below) the competitive level, or otherwise injure competition,” *id.*

Authenticom has made plausible factual allegations as to both elements. Indeed, the Court has already found that Authenticom “made the requisite likelihood of success showing” on the merits, Op. 16, with respect to the exclusive dealing claim. Authenticom therefore has necessarily established that this claim is plausible on the face of the Complaint. *See supra* p. 21.

1. Defendants’ Exclusive Dealing Terms Foreclose Authenticom from a Substantial Portion of the Data Integration Market

1. “Courts typically require a plaintiff to make an initial showing of foreclosure from competing in at least 30 to 40 percent of a market to proceed with a claim.” *Methodist Health Servs. Corp. v. OSF Healthcare Sys.*, 2016 WL 5817176, at *8 (C.D. Ill. Sept. 30, 2016), *aff’d*, 859 F.3d 408 (7th Cir. 2017); *see also, e.g., United States v. Microsoft Corp.*, 253 F.3d 34, 70 (D.C. Cir. 2001) (per curiam) (holding “roughly 40% or 50%” foreclosure of competition sufficient). Defendants’ exclusive dealing meets this standard – and neither CDK nor Reynolds argues otherwise. As this Court already found, Defendants’ exclusive dealing arrangements with vendors “effectively cut [Authenticom] out of the data integration market,” Op. 15, because the agreements prevent or effectively prevent dealers and vendors from working with Authenticom. *See supra* pp.14-15; Compl. ¶¶ 149, 157-158, 173, 175-177. And each of the Defendants accounts for 30 percent or more of the market; between them, CDK and Reynolds account for 75 percent of the market if judged by dealership rooftops (and upwards of 90 percent if judged by car sales). Compl. ¶ 33.

2. CDK contends (at 17) that no competition has been foreclosed because “3PA is not a competing data integrator; it is a managed interface that is integral to CDK’s DMS.” But Authenticom has made ample allegations – and adduced evidence consistent with those

allegations – that, from the perspective of vendors and dealers, Authenticom’s service is reasonably interchangeable with 3PA (on the CDK system) and RCI (on the Reynolds system), regardless of the marketing terminology CDK uses to describe its service. Data integration services are sold separately from the DMS, to different customers – with the DMS sold to dealers and data integration sold to vendors as well – and are subject to distinct demand. *See Compl. ¶ 63* (“the data integration market has its own supply and demand curves separate and apart from the DMS Market”); *see also id. ¶¶ 58, 76; [REDACTED]* [REDACTED]; Dkt. 106-17, at 9 (CDK’s 2015 10-K referring to data integration “as a stand-alone product” from “the core Dealer Management System”); *see also Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 19 (1984), *abrogated on other grounds by Illinois Tool Works Inc. v. Indep. Ink, Inc.*, 547 U.S. 28 (2006).

Consistent with those allegations, vendor testimony at the preliminary injunction hearing established that, from the consumer perspective, data integration provided by Authenticom and Defendants are indistinguishable. *See* Dkt. 165 (37:24-25, 38:1-2); *id.* (63:3-17, 67:19-25, 68:1-2) (absent restraints, vendors would purchase data integration from Authenticom rather than CDK or Reynolds); *see Reifert v. S. Cent. Wis. MLS Corp.*, 450 F.3d 312, 318 (7th Cir. 2006) (“Products and services are in the same market when they are good substitutes for one another.”); *ABS Global, Inc. v. Inguran, LLC*, 2016 WL 3963246, at *12 (W.D. Wis. July 21, 2016) (“A relevant market is comprised of those commodities reasonably interchangeable by consumers for the same purposes[.]”).

CDK’s own internal documents recognize that – in the absence of restraints – vendors would use independent integrators rather than [REDACTED]. And,

through its DMI and IntegraLink subsidiaries, CDK itself sells data integration on non-CDK DMS systems. Compl. ¶¶ 58, 71, 88-95.

Authenticom has plausibly alleged a “market for data integration services” – as this Court has already found at the preliminary injunction stage. Op. 9. Whether a jury will ultimately credit Authenticom’s alleged data integration market is a “deeply fact-intensive inquiry” for another day and certainly not appropriate to resolve on a Rule 12(b)(6) motion. *Ploss v. Kraft Foods Grp., Inc.*, 197 F. Supp. 3d 1037, 1070 (N.D. Ill. 2016).

Reynolds argues (at 44) that the Complaint fails to state a claim for exclusive dealing because Authenticom can continue to serve dealers that use DMS providers other than CDK and Reynolds. But antitrust law requires *substantial* foreclosure, not *complete* foreclosure. As explained above, 30 percent market foreclosure is sufficient as a matter of law. *See supra* p. 27.

2. The Effect of Defendants’ Exclusive Dealing Terms Has Been Supra-Competitive Pricing and Reduced Output

1. Authenticom has sufficiently alleged that the “effect of the exclusion[s]” imposed by Defendants has been to “raise prices above (and therefore reduce output below) the competitive level, or otherwise injure competition.” *Roland Mach.*, 749 F.2d at 394. This element is intensely factual in nature; to survive a Rule 12(b)(6) motion, it is sufficient for Authenticom to plausibly allege an injury to competition as shown by, among other things, increase in prices or reduction in output. *See, e.g., King Drug Co. of Florence, Inc. v. SmithKline Beecham Corp.*, 791 F.3d 388, 412 (3d Cir. 2015), *cert. denied*, 137 S. Ct. 446 (2016).

Authenticom has plausibly alleged that the exclusive dealing has raised prices above the competitive level. Compl. ¶¶ 214- 225, 257; *see* Op. 15-16. That finding was supported by undisputed evidence of drastic price increases in the wake of Defendants’ collusion, and was clearly alleged in the Complaint. *See* Op. 9-10; Compl. ¶¶ 214-225, 257. CDK charged one

vendor \$160 per dealer per month in 2014 (before exclusive dealing), and \$735 in July 2017 (after exclusive dealing), without any quality improvements. *See* Dkt. 165 (61:23-62:23); Compl. ¶ 218. Similarly, since 2011, Reynolds has increased monthly prices on another vendor from \$247 to \$893. *See* Dkt. 165 (32:16-33:7); Compl. ¶ 220. Although this pricing data was “not comprehensive,” Op. 9, that was largely because the parties with access to such data (CDK and Reynolds) did not present it. *See Int’l Union, UAW v. NLRB*, 459 F.2d 1329, 1335-38 (D.C. Cir. 1972) (drawing adverse inferences under such circumstances is a matter of “common sense”). Discovery will shed further light on the magnitude of Defendants’ price increases.

Authenticom has alleged (and shown) not only that Defendants have raised prices, but those prices vastly exceed competitive levels. *See* Compl. ¶¶ 214-25, 257. Specifically, competitive independent data integrators like Authenticom charge as little as \$30 per dealer per month – for a superior product – compared to the Defendants’ prices that were more than 20 times higher. *See supra* p. 16.

Further, the Complaint alleges that Defendants’ restraints and anticompetitive conduct reduced output, a natural consequence of such a large increase in prices. *See* Compl. ¶¶ 226-31. Consistent with the allegations of reduced output, vendors testified at the preliminary injunction hearing that Defendants’ price increases forced them to stop producing applications, including applications that increase consumer safety by notifying consumers of product recalls on older cars. *See* Dkt. 162 (188:23-189:5, 192:3-195:21); Dkt. 165 (35:14-20, 44:1-45:3). Two vendors testified that – for certain software applications – Defendants charge more for access to the necessary basic dealer data than the vendor charges the dealership for the application itself. *Id.*

2. In response to Authenticom’s allegations of competitive harm, Defendants argue (CDK Br. 18-20; Reynolds Br. 46-47) that the Complaint fails to plausibly allege a lack of

procompetitive justifications. But Authenticom has alleged a *prima facie* rule of reason case by plausibly alleging an increase in prices and a reduction in output. *E.g., West Penn Allegheny Health Sys., Inc. v. UPMC*, 627 F.3d 85, 100 (3d Cir. 2010) (complaint need only allege “anticompetitive effects in the relevant markets”). That shifts the burden to Defendants, which can attempt to prove, by a preponderance of the evidence, a business justification or that competitive benefits outweigh the higher prices and reduced output. *See* Model Jury Instructions in Civil Antitrust Cases, Instruction 3C, Rule of Reason – Evidence of Competitive Benefits (citing cases). How the jury will ultimately evaluate the competing evidence has no bearing on the sufficiency of Authenticom’s claims for relief at this stage.

In any event, Defendants rely on two unsupported theories to justify their elimination of competition and drastic price hikes: (1) that their conduct was justified by a need for enhanced security, and (2) that their contracts and technological interference constitute product design choices. Both arguments are belied by the allegations in the Complaint and the evidence adduced at the preliminary injunction hearing.

a. Although “plausible” in theory, Op. 18, Defendants’ security rationale is largely a pretext, as the Complaint alleges. Compl. ¶ 236; *see also* Op. 18-19. CDK’s own documents explain that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ These “damning internal documents” are “powerful evidence that [the] procompetitive justifications are ‘merely pretextual.’” *McWane, Inc. v. FTC*, 783 F.3d 814, 841-42 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 1452 (2016).

Moreover, Defendants' practice of selectively allowing competitive data integration when it serves their business interests undermines their security rationale. *See* Op. 2, 19; Compl. ¶ 237. Reynolds "whitelists" Authenticom's access to Reynolds' DMS for the Penske Automotive Group (the largest dealer group in the nation), Jaguar, and BMW, among others. *See* Dkt. 147-17; Dkt. 147-21; Dkt. 164 (127-33); Dkt. 163 (86-88); PHX-159. Reynolds also "whitelisted" CDK's access to Reynolds' DMS for the five-year "wind down" period in the February 2015 agreement. *See* Op. 16; Dkt. 163 (36-37, 69-70, 73-74). CDK meanwhile operates two data integrators – DMI and IntegraLink – that screen-scrape data from Reynolds' DMS (pursuant to the "wind down") and other providers' DMS. *See* Compl. ¶¶ 89-95, 144, 204. Defendants also use Authenticom's data integration services for their applications. *See* Dkt. 164 (120-121).

In addition, the Complaint alleges (and evidence establishes) that Authenticom is secure. Op. 4; Compl. ¶ 240. In its 15-year history, Authenticom has never had a data breach; its firewall has never been compromised; it has never even had a reportable security incident. *See* Compl. ¶ 240; Op. 18; Dkt. 164 (114). Authenticom uses Microsoft Azure, a secure cloud technology utilized by numerous large corporations and the U.S. government. *See* Compl. ¶¶ 84, 240; Op. 4; Dkt. 163 (185) (CDK's Vice President for Data Services testifying Azure is secure). Authenticom also uses best practices for data transparency (disclosing how data is used) and data minimization (sharing data only with those needing access). *See* Dkt. 162 (68-73). Authenticom does not "access data beyond the legitimate needs of its customers, vendors and dealers." Op. 18. And Authenticom allows dealers to control specifically the data that is sent to each vendor and to monitor where data has been sent. *See* Compl. ¶ 78; Op. 4; Dkt. 164 (92-101) (demonstration of DealerVault). Defendants' own security expert testified "when we talk about

transparency, DealerVault . . . is good. That's an impressive piece of technology." Dkt. 162 (134:23-25).

The methods by which Authenticom retrieves data from the DMS are also secure. Authenticom retrieves data from the DMS in the same manner that a dealer employee would retrieve that data. Compl. ¶ 55; *see* Dkt. 164 (108:15-17) ("[W]e utilize the application layer of the DMS system just like an employee would."). The only difference is that, instead of an employee manually retrieving data, Authenticom automates the process through screen-scraping. Compl. ¶¶ 55, 237-241; *see* Dkt. 164 (108:17-19) ("Essentially, we're an employee at the dealership typing in the data request only we have very fast fingers."). At the preliminary injunction hearing, Defendants mustered "no evidence that Authenticom's automated access was less secure than manual access by dealer employees." Op. 18.

b. The evidence is likewise inconsistent with the argument (CDK Br. 19-20; Reynolds Br. 33-35, 46) that Defendants' policy of blocking independent integrators is a product design choice that is immune from antitrust scrutiny. As the Complaint alleges, the current design of both the Reynolds and CDK DMS allows third-party access to dealer data. Indeed, both Reynolds and CDK continue to permit third-party access to their systems (including by Authenticom) when it is in their business interest to do so. *See* Compl. ¶ 144; Op. 16 ("Reynolds allows significant exceptions by 'whitelisting' certain third parties that it allows to access its system, most notably DMI, CDK's third-party integrator."); Dkt. 165 (60:21-22) ("Q: So I'd asked did CDK block SIS as well? A: No, they didn't."); Dkt. 164 (127:13-16), Dkt. 164 (130:16-131:15) (Reynolds-authorized access to dealer systems).

Allied Orthopedic Appliances Inc. v. Tyco Health Care Grp. LP, 592 F.3d 991 (9th Cir. 2010), thus does not support Defendants, not only because the gravamen of Authenticom's

Complaint has little to do with product design but also because the product design change at issue in *Allied Orthopedic* was not like any purported design feature at issue here. That case “stand[s] for the uncontroversial proposition that product improvement *by itself* does not violate Section 2.” *Id.* at 999. (emphasis added). But even a product improvement does not immunize “associated conduct” that is anticompetitive, such as the exclusive dealing arrangements here. *Id.*; *see id.* at 996-98 (analyzing separately the lawfulness of exclusive dealing arrangements and product design changes).

Even if Authenticom’s claims were properly characterized as challenging a “design choice,” Defendants’ conduct would still be subject to antitrust scrutiny: where a company with market power implements design changes that offer no benefit to consumers while foreclosing competition, it violates the Sherman Act. *See, e.g., New York ex rel. Schneiderman v. Actavis PLC*, 787 F.3d 638, 652-58 (2nd Cir. 2015); *Microsoft*, 253 F.3d at 65-66; *C.R. Bard, Inc. v. M3 Sys., Inc.*, 157 F.3d 1340, 1382-83 (Fed. Cir. 1998). That is what occurred here. Defendants’ blocking practices excluded competition without benefits to consumers. *See supra* pp. 16-18. By contrast, in *Allied Orthopedic* there was “[u]ndisputed [e]vidence that [the design change] [w]as an [i]mprovement.” 592 F.3d at 1000-02.

C. The Complaint Alleges Unlawful Tying

1. CDK's and Reynolds' vertical agreements with dealers also constitute unlawful tying in violation of Section 1 of the Sherman Act. A tying arrangement is an agreement by a party to sell one product – the “tying product” – only on condition that the buyer also purchase or agree not to buy from another supplier a second product – the “tied product.” *Eastman Kodak*, 504 U.S. at 461-62. Such arrangements are unlawful where sellers exploit their market power over one product to force unwilling buyers to deal exclusively with the seller in the market for another separate product. *See Jefferson Parish*, 466 U.S. at 12; *Northern Pac. Ry. Co. v. United States*, 356 U.S. 1, 6 (1958); *Times-Picayune Publ'g Co. v. United States*, 345 U.S. 594, 605 (1953).

Defendants concede that their contracts with dealers condition the purchase of DMS software (the tying product) on the dealers' agreement to use only Defendants' integration services (the tied product). That condition forces dealers and the vendors they contract with to obtain data integration services from Defendants, because vendors can gain access to the dealer data necessary to provide their services only by means of a data integration provider authorized by the dealer. *See* Compl. ¶¶ 150-152, 154, 264.

That arrangement constitutes unlawful tying. *See Jefferson Parish*, 466 U.S. at 12 (“[T]he essential characteristic of . . . tying . . . lies in the seller's exploitation of its control over the tying product to force the buyer into the purchase of a tied product that the buyer . . . might have preferred to purchase elsewhere on different terms. When such ‘forcing’ is present, competition on the merits in the market for the tied item is restrained and the Sherman Act is violated.”); *Eastman Kodak*, 504 U.S. at 461-63 (noting evidence “that Kodak would sell parts to third parties only if they agreed not to buy service from [independent service organizations]” as proof of a tying arrangement); *Northern Pac. Ry.*, 356 U.S. at 5-6 (“[A] tying arrangement may be defined

as an agreement by a party to sell one product but only on the condition that the buyer. . . agrees that he will not purchase that product from any other supplier.”).

2. Defendants’ tying is unlawful per se because: (1) two separate “products” are involved; (2) each Defendant has sufficient economic power in the tying market to appreciably restrain free competition in the market for the tied product; and (3) the arrangements each affect a substantial volume of interstate commerce.⁴ *See Reifert v. S. Cent. Wis. MLS Corp.*, 450 F.3d 312, 316 (7th Cir. 2006); *Eastman Kodak*, 504 U.S. at 461-62; *Jefferson Parish*, 466 U.S. at 12-18.

First, Authenticom has alleged that DMS systems are a separate and distinct product from dealer data integration services. Whether two products are distinct for the purposes of a tying claim “turns not on the functional relation between them, but rather on the character of the demand for the two items.” *Jefferson Parish*, 466 U.S. at 19. The market demonstrates such separate demand here. *See* Compl. ¶¶ 28-37 (the DMS market); *id.* ¶¶ 47-67 (the Dealer Data Integration Market). Authenticom and other integration providers have offered dealer data integration services without also offering DMS software, *see id.* ¶ 54, and Defendants themselves have separate data integration products distinct from their DMS products, *id.* ¶ 58. That consumer demand supports the separate furnishing of these services is sufficient to demonstrate the existence of separate product markets. *See Eastman Kodak*, 504 U.S. at 462 (“For service and parts to be considered two distinct products,” so as to support a “tying

⁴ Even if these three factors cannot be met, the accused tying arrangement may still be found unlawful under the rule of reason. *See Carl Sandburg Vill. Condo. Ass’n No. 1 v. First Condo. Dev. Co.*, 758 F.2d 203, 210 (7th Cir. 1985) (“[A] plaintiff’s failure to state a *per se* illegal antitrust claim does not necessarily prove fatal to his case if he can state a claim under the rule of reason.”). As shown above, *supra* Part III.A.1, the complaint properly alleges a claim under the rule of reason as well.

arrangement” claim “there must be sufficient consumer demand so that it is efficient for a firm to provide service separately from parts.”).

Second, as discussed above, CDK and Reynolds each have market power in the market for DMS software (the tying product). “[T]here are two ways of proving market power” – either (1) “through direct evidence of anticompetitive effects” or (2) “by proving relevant product and geographic markets and by showing that the defendant’s share exceeds whatever threshold is important for the practice in the case.” *Toys “R” Us*, 221 F.3d at 937.

Here, there is direct evidence that Defendants have “the power to affect price or exclude competition” in the DMS market. *United States v. Visa U.S.A., Inc.*, 344 F.3d 229, 239 (2d Cir. 2003); *see also K.M.B. Warehouse Distrib., Inc. v. Walker Mfg. Co.*, 61 F.3d 123, 129 (2d Cir. 1995); *42nd Parallel N. v. E St. Denim Co.*, 286 F.3d 401, 405-06 (7th Cir. 2002) (“The key inquiry in a market power analysis is whether the defendant has the ability to raise prices without losing its business.”). Defendants have successfully imposed significant price increases for DMS software – untethered to costs – without losing many dealers to rivals. *See Compl. ¶¶ 214-225, 257* (Reynolds’ and CDK’s DMS contracts have price-escalation clauses with automatic yearly price increases). Where a defendant has in fact controlled prices or excluded competition, “no more elaborate market analysis [is] necessary.” *Toys “R” Us*, 221 F.3d at 937.

Furthermore, the market conditions alleged in the Complaint confirm that each Defendant controls a sufficient portion of the market to support a finding of market power for purposes of a tying claim. *See Compl. ¶ 33* (CDK controls approximately 45% of dealer rooftops, Reynolds approximately 30%); *see, e.g., Hardy v. City Optical Inc.*, 39 F.3d 765, 767 (7th Cir. 1994) (recognizing “30 percent or more” as “the minimum market share from which the market power

required to be shown at the threshold of a tying case can be inferred.”). Defendants’ market power is enhanced by the high barriers to entry into the market and the high costs of switching suppliers. Compl. ¶¶ 28, 38-45.

Third, Defendants’ tying arrangements – given their large market shares – have affected a “not-insubstantial” volume of commerce. *Reifert*, 450 F.3d at 318.

2. Defendants argue (CDK Br. 14-16; Reynolds Br. 42-43), that vendors, rather than dealers, directly pay for integration services, and therefore the customers are different for the tying (DMS) and tied (integration services) products. But the Complaint alleges that dealers – not vendors – make the decision about which integrators will be permitted access to their system. *See* Compl. ¶¶ 5, 16. Without express dealer authorization, integrators cannot access a dealer’s data. *Id.* ¶ 55. Dealers are therefore the relevant targets of Defendants’ tying arrangement. *Id.* It does not matter that vendors pay the integration service fees because the dealers still control the selection of integration services and are thus the subjects of the illegal “forcing,” which is what matters for purposes of a tying claim. *See Dos Santos v. Columbus-Cuneo-Cabrini Med. Ctr.*, 684 F.2d 1346, 1354 (7th Cir. 1982) (hospital, rather than patient, may be relevant purchaser for antitrust purposes because the “patient generally takes no part in the selection of a particular anesthesiologist,” even though the hospital may bear none of the costs). And that conclusion gains added force from the fact that the dealers ultimately bear the cost of integration services indirectly through the cost of the applications they purchase from vendors. *See* Compl. ¶¶ 224, 228; *see also* Dkt. 86, ¶ 253 (Defendants acknowledging that “some vendors pass through some” or “all” of “their integration fees”); *see American Needle*, 560 U.S. at 193 (“The Sherman Act . . . is aimed at substance rather than form.”) (quotations and citations omitted).

II. Authenticom Has Stated a Plausible Monopolization Claim Under Section 2 of the Sherman Act

“The offense of monopoly under § 2 of the Sherman Act has two elements: (1) the possession of monopoly power in [a] relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.” *Briggs & Stratton Corp. v. Kohler Co.*, 405 F. Supp. 2d 986, 990 (W.D. Wis. 2005). Authenticom has pleaded both elements.

A. The Complaint Pleads That Defendants Have Market Power in Their Respective Data Integration Aftermarkets

Defendants incorrectly assert that Authenticom has not alleged a plausible antitrust after-market under *Eastman Kodak*. But Authenticom, consistent with the principles articulated in that case, plausibly alleges that CDK and Reynolds each possess market power in the brand-specific aftermarkets for dealer data integration on their respective platforms. Compl. ¶¶ 111-16.

Eastman Kodak recognized that antitrust markets may appropriately be divided into brand-specific “sub-markets” (here, data integration on CDK’s and Reynolds’ respective platforms) where “significant information and switching costs” impede consumers from switching between brands in the primary market (here, the DMS market). *Eastman Kodak*, 504 U.S. at 476 (“If the cost of switching is high, consumers who already have purchased the equipment, and are thus ‘locked in,’ will tolerate some level of service-price increases before changing equipment brands”).

The markets alleged here fit squarely within the principles articulated in *Eastman Kodak*: Authenticom has alleged enormous switching and information costs in the DMS market, which have allowed Reynolds and CDK to “profitably . . . maintain supracompetitive prices in the

aftermarket” for data integration on their respective platforms. *Eastman Kodak*, 504 U.S. at 476.⁵

a. Switching Costs. Authenticom has alleged significant switching costs in the primary DMS market. CDK and Reynolds require dealers to sign long term contracts of five to seven years in length. Compl. ¶ 39. Beyond the contract length, dealers invest substantially in their DMSs, the “mission-critical enterprise software that manages nearly every function of a dealer’s business.” *Id.* ¶ 3. Once a dealer builds its operations on a particular DMS platform – and trains its workforce – it is disruptive and expensive to switch, as doing so “changes nearly every process that a dealer uses to operate.” *Id.* ¶¶ 40-42; Dkt. 56 (Maas Decl. ¶ 7). One dealer said switching is akin to a “heart transplant,” and some of the nation’s largest and most sophisticated auto dealerships have tried and failed to switch DMS providers. Compl. ¶ 40. Defendants have added to the inherent barriers to switching through their anticompetitive conduct – including by preventing dealers from transferring their historical data to a new DMS system. *Id.* ¶¶ 43-44. As CDK’s CEO recently acknowledged, “switching DMS providers can be very difficult. It [is] quite a process [to] change and takes time, which is part of the reason that many dealers are hesitant to switch.” *Id.* ¶ 40.

Consequently, the *average* DMS tenure is more than 20 years. Compl. ¶ 40; Dkt. 146, ¶ 15. Defendants’ own pleadings in this case have stated [REDACTED]

⁵ In *Eastman Kodak*, there were two relevant markets: the primary market for photocopiers and micrographic equipment and a derivative aftermarket for service and replacement parts for such equipment. 504 U.S. at 463. The plaintiffs alleged that the market for servicing Kodak-brand equipment was a distinct aftermarket and cognizable under the Sherman Act. The Court agreed. *Id.* at 486. As the Court explained, “significant information and switching costs . . . could create a less responsive connection between service and parts prices and equipment sales,” permitting Kodak to exert market power in the service and parts aftermarket even though there was competition in the primary market for office equipment. *Id.* at 473.

Defendants' own calculations, [REDACTED]

[REDACTED] The DMS market is thus extraordinarily sticky. *Eastman Kodak*, 504 U.S. at 477 (switching costs include "heavy initial outlay" for copy machines and other brand-specific investment); *see also Collins Inkjet Corp. v. Eastman Kodak Co.*, 2014 WL 11516553, at *9 (S.D. Ohio Mar. 21, 2014) (holding plaintiff established likely *Eastman Kodak* aftermarket under preliminary injunction standard, where office printers had a lifespan of 10-20 years and buyers "have invested time and money into training their employees" on the system), *aff'd*, 781 F.3d 264 (6th Cir. 2015).

These allegations are sufficient to state a claim. *See, e.g., Red Lion Med. Safety, Inc. v. Ohmeda, Inc.*, 63 F. Supp. 2d 1218, 1232 (E.D. Cal. 1999) (holding that where there is competing evidence on lock-in, "disputed issues for trial" preclude *summary judgment*).

b. Information Costs. Authenticom has also alleged substantial "information costs," *Eastman Kodak*, 504 U.S. at 477, that further impede switching between DMS brands. Vendors, not dealers, directly pay for data integration. Compl. ¶ 59. Taking full advantage of this disjunction, Defendants impose price secrecy provisions on vendors, which are explicitly designed to prevent dealers from learning how much Defendants charge for data integration. Compl. ¶¶ 166-170. Defendants' price secrecy provisions ensure a "less responsive connection," 504 U.S. at 474, between supracompetitive prices in the data integration aftermarket and competition in the DMS market.

[REDACTED] As for

Reynolds, Mr. Schaefer admitted that its price secrecy provision is designed to prevent dealers from negotiating over the cost of data integration. Dkt. 163 (51:11-15) (If dealers knew how much Reynolds charges vendors for data integration, “what happens is they get into a comparison” and Mr. Schaefer “do[es]n’t have time to do all that and put it together and negotiate. Because, you know, car dealers and vendors, their strength is negotiations, and so they want to take all of the information they can get and come hit me.”).

These allegations (and evidence) of switching and information costs allege lock-in under *Eastman Kodak*.

Schor v. Abbott Labs., 457 F.3d 608 (7th Cir. 2006) – upon which Reynolds relies (at 36-37) – supports Authenticom. In *Schor*, the Seventh Circuit noted that, under *Eastman Kodak*, firms with market power may not deal in “complementary products” “in ways that take advantage of customers’ sunk costs,” *id.* at 614 – for example, by switching business models. That is what Authenticom alleges: Defendants have exploited dealers’ sunk costs with respect to their DMS choice by seizing control over the dealers’ data and charging monopoly prices for vendors to access it. And, unlike in *Schor*, Reynolds imposes price secrecy provisions that conceal the true life cycle cost of the Reynolds DMS. Compl. ¶¶ 166-170.

c. Defendants argue (CDK Br. 21; Reynolds Br. 38) that the presence of an “unauthorized access” provision in their DMS contracts with dealers negates, as a matter of law, Authenticom’s *Eastman Kodak* claim.⁶ That is incorrect.

⁶ Reynolds also argues (at 38) that Authenticom failed to plead Reynolds has monopoly power in the DMS market. But Authenticom is not alleging that Reynolds has monopolized the DMS market – just as the plaintiff in *Eastman Kodak* did not need to allege that Kodak had monopolized the market for photocopiers. Rather, Authenticom alleges that Reynolds has

As an initial matter, far from prohibiting third-party access, CDK’s DMS contracts expressly allow dealers to authorize “agents” to access the DMS on the dealers’ behalf, and actively marketed its DMS product as allowing dealers to use independent integrators. *See supra* pp. 6, 15. There is nothing in the CDK DMS contract that would have put dealers on notice that CDK – after luring dealers into long-term contracts – planned to make an abrupt about-face, exclude third-party integrators, and force vendors to use CDK’s in-house data integration services (at steeply inflated prices).

Moreover, whatever the contracts say or mean, Authenticom has alleged that Defendants’ actual real-world policies with regard to third-party integration services changed after the dealers were already locked-in. Compl. ¶¶ 188-189. Defendants’ own cases recognize that a company’s “change in policy” is a “crucial factor” in the *Eastman Kodak* analysis. *See PSI Repair Servs., Inc. v. Honeywell, Inc.*, 104 F.3d 811, 820 (6th Cir. 1997) (“By changing its policy after its customers were ‘locked in,’ Kodak took advantage of the fact that its customers lacked the information to anticipate this change.”). Until 2015, CDK repeatedly – and publicly – supported independent data integration and provided such dealer-authorized integration services itself, including on the Reynolds system. *See supra* p. 6; Dkt. 54 (Korp. Decl. ¶ 22) (“When we entered into our long-term DMS contract with CDK, we had no idea CDK would take this position and would begin disabling and blocking our ability to provide vendors and other third parties of our choosing with access to our own data.”). Reynolds, too, changed its policy with regard to enforcement of its DMS agreements – with tepid blocking in 2009, followed by more

monopolized the market for data integration services on the Reynolds DMS. *See* Compl. ¶¶ 111-16.

aggressive blocking coupled with astronomical data integration price hikes since 2013.⁷ Op. 5.

With the average DMS client tenure exceeding 20 years, most dealers were “locked in” long before Defendants’ recent policy changes.

Furthermore, courts recognize *Eastman Kodak* claims notwithstanding an “unauthorized access” provision in the initial contract. In *Datel Holdings, Ltd. v. Microsoft Corp.*, for example, the initial contract gave the manufacturer (Microsoft) the right to prohibit “unauthorized” accessories and hardware on its Xbox game system. 712 F. Supp. 2d. 974, 988-90 (N.D. Cal. 2010). The court rejected Microsoft’s attempt to dismiss the *Eastman Kodak* claim on this basis, because it was a factual question as to whether a “customer purchasing an Xbox 360 console would understand the contract as prohibiting unauthorized accessories.” *Id.* at 989; *see also Burda v. Wendy’s Int’l, Inc.*, 659 F. Supp. 2d 928, 935 (S.D. Ohio 2009) (*Eastman Kodak* claim cognizable despite “authorized supplier” provision in initial franchise agreement); *Avaya Inc. v. Telecom Labs, Inc.*, 2014 WL 2940455, at *6 (D. N.J. June 30, 2014) (jury found for plaintiff on *Eastman Kodak* claim despite contract-based ban of “unauthorized” service providers for Avaya-brand phones). The same holds true here.

CDK’s reliance on *Queen City Pizza, Inc. v. Domino’s Pizza, Inc.*, 124 F.3d 430 (3d Cir. 1997), is misplaced. There, plaintiff was a Domino’s Pizza franchisee that agreed to use pizza

⁷ Reynolds claims (at 38-39) that, since 2007, “every dealership” that uses the Reynolds DMS has known about its “closed” nature. That is not accurate: on the contrary, the Complaint alleges that Reynolds only began its most significant blocking efforts in 2013, on a vendor-by-vendor basis, with an accompanying June 2013 public announcement. Compl. ¶ 189. Most Reynolds customers began using the Reynolds DMS long before 2013 (or 2007), given the average client tenure is 20 years; those dealers were thus “locked in” before Reynolds began its current policy of blocking. Ultimately, the question of when dealers knew Reynolds planned to lock out third-party integrators and force vendors to use RCI at steeply inflated prices is a factual one that cannot be resolved on the pleadings. *See Datel Holdings Ltd. v. Microsoft Corp.*, 712 F. Supp. 2d. 974, 988-90 (N.D. Cal. 2010).

ingredients “exclusively from [Domino’s] or from approved suppliers or distributors” in its franchise agreement. *Id.* at 433. The Third Circuit rejected the plaintiff’s *Eastman Kodak* theory because there was no dispute that other pizza ingredients were reasonably interchangeable with the Domino’s-approved ingredients; the sole reason those alternatives could not be used was because plaintiffs had agreed with Domino’s that they would not use them. *Id.* at 438-49. Here, by contrast, the data integration services provided to a particular dealer must be compatible with its particular DMS – in this regard, integration services are closely analogous to the brand-specific service at issue in *Eastman Kodak*. Just as competition in the market for copiers did not necessarily protect the owners of Kodak-brand copiers from the exercise of market power in the market for service, *see Schor*, 457 F.3d at 614, so too any potential competition in the market for DMS service does not protect dealers on a particular DMS from the exercise of market power in the market for data integration service. *See also Blizzard Entm’t Inc. v. Ceiling Fan Software LLC*, 941 F. Supp. 2d 1227, 1235 (C.D. Cal. 2013) (The “inquiry is whether the market power is derived from contractual *provisions* it obtained in the initial market, as in *Queen City Pizza*, or through the contractual *relationship* it has with its consumers, as in *Eastman Kodak*.”).

* * * * *

As *Eastman Kodak* recognized, the “proper market definition in this case can be determined only after a factual inquiry into the ‘commercial realities’ faced by consumers.” 504 U.S. at 482; *Wilk v. Am. Med. Ass’n*, 895 F.2d 352, 360 (7th Cir. 1990) (“Whether market power exists in an appropriately defined market is a fact-bound question.”). Defendants offer no basis to short-circuit that factual inquiry before discovery has even begun. *See In re Dairy Farmers of Am., Inc. Cheese Antitrust Litig.*, 767 F. Supp. 2d 880, 901 (N.D. Ill. 2011) (“[B]ecause market definition is a deeply fact-intensive inquiry, courts hesitate to grant motions to dismiss for failure

to plead a relevant product market.””) (quoting *Todd v. Exxon Corp.*, 275 F.3d 191, 199-200 (2d Cir. 2001) (Sotomayor, J.)).

B. The Complaint Adequately Pleads That Defendants Acquired and Maintain Their Market Power Through Anticompetitive Means

Authenticom has plausibly alleged that Defendants acquired or maintain “monopoly power through anticompetitive or exclusionary means.” *Lerma v. Univision Commc’ns, Inc.*, 52 F. Supp. 2d 1011, 1018 (E.D. Wis. 1999). A monopolist abuses its power by using it to “foreclose competition, gain a competitive advantage, or destroy a competitor.” *Id.* at 1019 (citing *Eastman Kodak*, 504 U.S. at 482-83).

Authenticom’s allegations (and evidence) which support Authenticom’s claims under Section 1 – that CDK and Reynolds entered into an unlawful horizontal market division agreement, conspired to exclude all other data integrators from the market, engaged in concerted activities to disrupt dealers’ access to third-party integration services, and imposed exclusive dealing arrangements and price secrecy provisions, *see supra* pp. 14-16 – are also sufficient to show that Defendants obtained and are maintaining their monopoly power through anticompetitive means. *See Gumwood HP Shopping Partners, L.P. v. Simon Prop. Grp., Inc.*, No. 3:11-CV-268 JD, 2013 WL 3214983, at *7 (N.D. Ind. Mar. 13, 2013) (“Where defendant has engaged in unlawful restraint of trade that would independently violate Section 1 of the Sherman Antitrust Act, it is well established that it also violates Section 2 if it acquires or maintains a monopoly by means of that restraint of trade.”); *ZF Meritor, LLC v. Eaton Corp.*, 696 F.3d 254, 271 (3d Cir. 2012) (“Exclusive dealing arrangements are of special concern when imposed by a monopolist.”); *Methodist Health Servs.*, 2016 WL 5817176, at *9 (it is anticompetitive for a “monopolist defendant” to “deploy[] exclusive contracts to limit completely their competitors’ ability to access the market”).

Defendants rely (CDK Br. 23-24; Reynolds Br. 27, 31-34) on *Trinko* to argue that their conduct was not anticompetitive, but that case does not support Defendants. Nothing in Authenticom’s Complaint seeks Defendants’ *cooperation* or requires a regime of “forced sharing.” *See* 540 U.S. at 408. Rather, Authenticom complains that Defendants block dealers and vendors from doing business with Authenticom. Unlike in *Trinko*, therefore, Authenticom challenges affirmative (and concerted) anticompetitive actions that Defendants have taken to interfere with the voluntary business relationships that Authenticom has forged with dealers and vendors who value Authenticom’s service over Defendants’ competing services.

Reynolds’ attempt (at 30-32) to shoehorn this case into the refusal-to-deal doctrine fares no better. That “doctrine targets only a discrete category of section 2 cases attacking a firm’s unilateral decisions about with whom it will deal and on what terms.” *Novell, Inc. v. Microsoft Corp.*, 731 F.3d 1064, 1076 (10th Cir. 2013) (Gorsuch, J.). It provides no safe haven for Defendants’ “affirmative[] interfer[ence] with [Authenticom’s] business activities.” *Id.* (citing *Conwood Co. v. U.S. Tobacco Co.*, 290 F.3d 768, 783-84 (6th Cir. 2002) (removal of rivals’ products from store shelves was anticompetitive)). Notably, Authenticom alleges, *inter alia*, that Defendants’ exclusive dealing restraints are exclusionary and anticompetitive – which goes to Defendants’ agreements with vendors and dealers, not any refusal to deal with Authenticom. *See Novell*, 731 F.3d at 1072 (distinguishing exclusive dealing from refusal to deal).

III. The Computer Fraud and Abuse Act Does Not Defeat Authenticom’s Claims

Defendants argue (CDK Br. 22-23; Reynolds Br. 9-21) that because they (selectively) block Authenticom’s access to their DMSs, any access not expressly permitted by Defendants would be without their authorization and would therefore violate the CFAA (and the Wisconsin Computer Crimes Act). Defendants claim this undermines Authenticom’s ability to claim antitrust injury. *Id.* But Defendants’ reliance on the CFAA provides no basis for dismissal of

Authenticom's antitrust claims for three reasons: (1) allegations of illegal conduct by Authenticom is not a defense to Defendants' antitrust violations; (2) the CFAA is not an antitrust immunity statute; and (3) Authenticom has not violated the CFAA because it only accesses the dealers' own data with the dealers' express authorization. (This last argument explains why Defendants' tortious interference defense is likewise unavailing at this stage.)

1. The legal premise of Defendants' antitrust injury argument is incorrect: the Supreme Court has made clear that claims that a plaintiff's business is illegal do not absolve defendants of antitrust liability due to the "overriding public policy in favor of competition" and the importance of private actions to deter violations. *Perma Life Mufflers, Inc. v. Int'l Parts Corp.*, 392 U.S. 134, 139 (1968). "[I]llegality is not to be recognized as a defense to an antitrust action when the illegal acts by the plaintiff are directed against the defendant. A wrongful act committed against one who violates the antitrust laws must not become a shield in the violator's hands against operation of the antitrust laws." *Memorex Corp. v. Int'l Bus. Machines Corp.*, 555 F.2d 1379, 1382 (9th Cir. 1977) (rejecting argument that plaintiff lacked standing because its business was built on trade secrets stolen from defendant); *see Pinto Trucking Serv., Inc. v. Motor Dispatch, Inc.*, 649 F.2d 530, 534 n.5 (7th Cir. 1981) ("Proof of the plaintiff's unrelated unlawful conduct is not a valid *in pari delicto* defense to an antitrust charge."); *Lamp Liquors, Inc. v. Adolph Coors Co.*, 563 F.2d 425, 431 (10th Cir. 1977). Reynolds' principal case, *Maltz v. Sax*, 134 F.2d 2 (7th Cir. 1943) – in addition to being distinguishable, as explained below – predates *Perma Life* and has been abrogated. *See Consolidated Exp., Inc. v. New York Shipping Ass'n, Inc.*, 602 F.2d 494, 526 n.21 (3d Cir. 1979) (recognizing abrogation), *rev'd on other grounds*, 448 U.S. 902 (1980); *see also Pinto Trucking*, 649 F.2d at 534 n.5.

2. The particular claim of illegality here – that Authenticom’s access to Defendants’ systems is unauthorized and therefore violates the CFAA – cannot deprive Authenticom of standing because it depends on whether Reynolds’ conduct violates the antitrust laws. As the court suggested in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62-63 (1st Cir. 2003) (Boudin, J.), “public policy” may “limit certain restrictions” on access to information stored on a computer. Here, if Defendants restricted access to their DMS pursuant to agreements that violate the Sherman Act – as Authenticom alleges (and the district court found a likelihood that Defendants did, Op. 14-16) – the invalidation of those unlawful restraints would, perforce, vitiate Defendants’ CFAA claim. The CFAA argument thus does nothing to detract from Authenticom’s antitrust standing. The particular claim of illegality here – that Authenticom’s access to Defendants’ systems is unauthorized and therefore violates the CFAA – cannot deprive Authenticom of standing because it depends on whether Defendants’ conduct violates the antitrust laws.

The recent district court decision in *hiQ Labs, Inc. v. LinkedIn Corporation*, 2017 WL 3473663 (N.D. Cal. Aug. 14, 2017), illustrates the point. hiQ is a data-analytics business that “scrapes” data from LinkedIn public profiles. *Id.* at *1. LinkedIn sent hiQ a cease-and-desist letter, alleging that its User Agreement prevented hiQ’s automated access and that “any future access of any kind” by hiQ on LinkedIn’s computer servers would be “without permission and without authorization from LinkedIn.” *Id.* at *2. LinkedIn thereafter implemented technological measures to block hiQ. *Id.*

hiQ moved for a preliminary injunction, alleging LinkedIn was engaging in unfair competition. The court granted the motion, rejecting LinkedIn’s argument that hiQ ran afoul of the CFAA. Under LinkedIn’s interpretation of the CFAA – like Defendants’ interpretation here

– it “would be free to revoke ‘authorization’ with respect to any person, at any time, for any reason, and invoke the CFAA for enforcement, potentially subjecting an Internet user to criminal, as well as civil, liability.” *Id.* at *6. The court rejected that theory, as it “would not leave any room for the consideration of either a [computer] owner’s reasons for denying authorization or an individual’s possible justification for ignoring such a denial.” *Id.* For the same reason, Defendants’ claim that the CFAA somehow privileges their conduct in denying dealers the ability to authorize Authenticom’s access – irrespective of whether that denial of access itself violates the antitrust laws – is incorrect.

Moreover, and more broadly, Seventh Circuit precedent suggests that the law significantly restricts the right of a database provider to include in licensing agreements restrictions on users’ freedom to share their own data – including on an automated basis. In *Assessment Techs. of Wis., LLC v. WIREdata, Inc.*, 350 F.3d 640, 642 (7th Cir. 2003), the plaintiff owned a database that stored a compilation of residential real-estate data collected and entered into the database by municipal property assessors. *Id.* at 647. The defendant extracted data for use by real-estate brokers with municipalities’ consent. The plaintiff argued that such access violated copyright law, but the Seventh Circuit rejected that claim. Instead, it held that the plaintiff had no right to stop municipalities from obtaining their own information from the database, including by authorizing third parties to do so. *See id.* at 648. And, although the court noted that the plaintiff in that case did not allege any breach of the licensing agreement between the plaintiff and the municipalities, the court suggested that an attempt to prevent the municipalities “from revealing *their own* data . . . might constitute copyright misuse.” *Id.* at 647-48. The court commented that it “would be appalling” if plaintiff’s attempt to “secrete the data in [a] copyrighted program” were permitted to succeed. *Id.* at 641-42.

These concerns are squarely implicated here. Authenticom accesses only dealer data and only with the dealer’s express authorization. Compl. ¶ 78. Indeed, as the Complaint alleges, both Defendants concede that dealers’ business and operational data belongs to the dealers. *See* Compl. ¶¶ 65-66. The allegations of the Complaint (along with the evidence adduced during the preliminary injunction hearing) strongly support the conclusion that the primary reason that Defendants closed their DMS systems was that it allowed them to exploit the value of dealer data – to the detriment of the dealers themselves. *See supra* p. 9. In a competitive market, that conduct would be punished. In the absence of effective competition, the conduct can inflict – and has inflicted here – significant harm on consumers and vendors.

Defendants gain no support from cases like *In re Canadian Import Antitrust Litig.*, 470 F.3d 785 (8th Cir. 2006), *Maltz v. Sax*, 134 F. 2d 2 (7th Cir. 1943), and *Bubis v. Blanton*, 885 F.2d 317 (6th Cir. 1989). Even assuming those cases are consistent with *Perma Life* and *Pinto Trucking* – *see Bubis*, 885 F.2d at 320 (Ryan, J., dissenting) – they involved businesses that were *independently* unlawful. *See Canadian Import*, 470 F.3d at 791 (trade restrictions “caused by the federal statutory and regulatory scheme adopted by the United States government, not by the conduct of the defendants”); *Maltz*, 134 F.2d at 5 (contraband gambling machines); *Bubis*, 885 F.2d at 320 (state liquor regulations). But where the claim of illegality is the flip-side of Authenticom’s antitrust claim, it cannot deprive Authenticom of antitrust standing. In this case, Defendants assert that Authenticom’s provision of data integration services runs afoul of the CFAA only to the extent that Defendants have blocked Authenticom from providing service to Defendants’ dealer customers. It is precisely that conduct that Authenticom’s Complaint challenges.

3. In any event, Authenticom does not violate the CFAA. With respect to CDK, its contracts with dealers expressly allow dealers to designate “employees and agents” to access the DMS on the dealers’ behalf. Dkt. 106-10, § 6 (emphasis added); Dkt. 163 (173-174). That is precisely what Authenticom does: it pulls data only to the extent specifically authorized by the dealer and on the dealer’s behalf. *See Compl. ¶ 78; Restatement (Third) of Agency § 1.01 (2006) (agent “act[s] on the principal’s behalf and subject to the principal’s control”).*

Reynolds’ dealer contracts do not expressly permit access by dealers’ agents, and Reynolds asserts that it disapproves of such access, but that does not change the result under a proper construction of the CFAA.⁸ When a dealer provides Authenticom credentials to log on to the DMS for the purpose of obtaining data that the dealer has the right to access, Authenticom has all the “authorization” it needs to access that data consistent with the CFAA. Reynolds’ contention that the dealer’s grant of permission to Authenticom violates its contracts may give rise to a civil dispute between the dealer and Reynolds, but it does not transform Authenticom’s access – at all times at the dealer’s behest – into a federal crime. *See AtPac, Inc. v. Aptitude Sols., Inc.*, 730 F. Supp. 2d 1174, 1180-81 (E.D. Cal. 2010) (holding that, “[s]imply put, a person cannot access a computer ‘without authorization’ if the gatekeeper has given them permission to use it” and holding third parties are not “liable under the CFAA for exploiting a licensee’s violation of its license agreement”).

Indeed, the CFAA focuses on the unauthorized access of computer systems to *obtain information*. *See* 18 U.S.C. § 1030(a)(2)(C) (“intentionally access[] a computer without

⁸ Although Defendants also cite the Wisconsin Computer Crimes Act, the only suggestion that the state statute provides a broader prohibition than the CFAA is the provision that prohibits “[d]isclos[ing] restricted access codes . . . to unauthorized persons.” Wis. Stat. § 943.70(2)(a)(6). Defendants do not claim that Authenticom improperly disclosed any “access codes” at all, let alone that the Complaint alleges such facts.

authorization or exceed[] authorized access, and thereby obtains . . . information from any protected computer”). Frequently the owner of the computer and the owner of the information will be one and the same. But here, while Defendants own the computer hardware, the dealer owns the only data that Authenticom accesses. It is more consistent with the statute’s language and purposes to conclude that if the owner of the information grants access, that authorization is legally sufficient, even if the computer owner objects. *See* Orin Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1178-79 (2016) (“If the agent accesses the account on the account holder’s behalf, the agent is acting in the place of the account holder and is authorized.”).

The division of data ownership and computer ownership present here makes Reynolds’ primary case – *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), *pet. for cert. pending*, No. 16-1105 (U.S. filed Mar. 9, 2017) – inapt. There, the data Power Ventures sought to access was “Facebook’s data” – not exclusively the user’s data. *Id.* at 1068 (“Power continued to access Facebook’s data and computers without Facebook’s permission”); *see also* *Facebook, Inc. v. Power Ventures, Inc.*, 2013 WL 5372341, at *1 (N.D. Cal. Sept. 25, 2013) (“Facebook complains that Defendants employ Facebook’s proprietary data without its permission by inducing Facebook users to provide their login information and then using that information to ‘scrape’ Facebook’s proprietary material.”). Moreover, Facebook maintained gatekeeping authority over its system by controlling the creation of usernames and passwords; by contrast, Defendants authorize dealers to create their own usernames and passwords to access the DMS. The court in *Facebook* thus had no occasion to address whether the user’s authorization would have been sufficient if Power Ventures had sought only to access the user’s data using credentials specifically created by the dealers themselves.

IV. Authenticom Has Stated a Plausible Claim for Tortious Interference

Under Wisconsin law, tortious interference with contractual relations has five elements: “(1) the plaintiff had a contract or prospective contractual relationship with a third party; (2) the defendant interfered with the relationship; (3) the interference was intentional; (4) a causal connection exists between the interference and the damages; and (5) the defendant was not justified or privileged to interfere.” *Burbank Grease Servs., LLC v. Sokolowski*, 717 N.W.2d 781, 796 (Wis. 2006).

Defendants challenge only elements (1) and (5). *First*, Reynolds (but not CDK) argues (at 47-48) that Authenticom’s contracts with dealers and vendors were unlawful under the CFAA and state statute and thus void. But, as explained above at pp. 48-53, Reynolds has not shown that the CFAA is implicated here.

Second, both Defendants argue (CDK Br. 25-26; Reynolds Br. 48) that their interference is justified under § 773 of the Restatement (Second) of Torts, which provides that in certain circumstances interference may be privileged when asserting “in good faith a legally protected interest.”⁹ Here, Defendants claim their interference was justified because Authenticom’s contracts were “illegal.” But Section 773 applies to a defendant only if “(1) he has a legally protected interest, and (2) in good faith asserts or threatens to protect it, and (3) the threat is to protect it by appropriate means.” *Id.* cmt. a. There is no legally protected interest in violating the antitrust laws, and Defendants’ reliance on § 773 is therefore misplaced. *See id.* § 767 cmt. c (“Conduct specifically in violation of statutory provisions . . . may for that reason make an interference improper. This may be true, for example, of conduct that is in violation of antitrust

⁹ Defendants bear the burden of proof on this defense. *See Finch v. Southside Lincoln-Mercury, Inc.*, 685 N.W.2d 154, 169 (Wis. Ct. App. 2004).

provisions or is in restraint of trade.”). Moreover, “the issue of justification [under § 773] is usually an issue of fact, with the test being what is reasonable conduct under the circumstances,” *Thiesing v. Dentsply Int’l, Inc.*, 748 F. Supp. 2d 932, 953-54 (E.D. Wis. 2010), and is therefore inappropriate for resolution on a motion to dismiss. *See also Metso Minerals Indus., Inc. v. FLSmidth-Excel LLC*, 2010 WL 55845, at *3 (E.D. Wis. Jan. 5, 2010) (“[I]ssues such as whether a party [asserting privileged under § 773] ‘acted in good faith’ . . . are almost exclusively questions of fact.”).

Finally, Reynolds is wrong (at 48) that the Complaint does not adequately allege false statements by Reynolds as a basis for liability. The Complaint alleges that Defendants – including Reynolds – told Authenticom’s dealers and vendors that Authenticom is not secure. Compl. ¶¶ 203, 235, 239-240. But that is untrue. Authenticom uses state-of-the art cybersecurity technology and has never had a breach. Compl. ¶ 240; *see supra* p. 8. Such alleged misrepresentations constitute improper interference with Authenticom’s customer contracts. *See Liebe v. City Fin. Co.*, 295 N.W.2d 16, 19 (Wis. Ct. App. 1980) (“[I]mproper means of interfering with contracts include transmission of false information.”).

CONCLUSION

Defendants’ motions to dismiss should be denied.

Dated: September 8, 2017

Respectfully submitted,

s/ Jennifer L. Gregor

Jennifer L. Gregor
Allison W. Reimann
GODFREY & KAHN, S.C.
One East Main Street, Suite 500
Madison, WI 53703
Phone: 608-257-3911
Fax: 608-257-0609
Email: jgregor@gklaw.com
areimann@gklaw.com

Michael N. Nemelka (*pro hac vice*)
Aaron M. Panner (*pro hac vice*)
David L. Schwarz (*pro hac vice*)
Kevin J. Miller (*pro hac vice*)
Derek T. Ho (*pro hac vice*)
Joshua Hafenbrack (*pro hac vice*)
Joanna T. Zhang (*pro hac vice*)
KELLOGG, HANSEN, TODD, FIGEL &
FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
Phone: (202) 326-7900
Fax: (202) 326-7999
Email: mnemelka@kellogghansen.com
apanner@kellogghansen.com
dschwarz@kellogghansen.com
kmiller@kellogghansen.com
dho@kellogghansen.com
jhafenbrack@kellogghansen.com
jzhang@kellogghansen.com

Attorneys for Plaintiff Authenticom, Inc.